ON THE ROOTS OF TRUNCATED HYPERGEOMETRIC SERIES OVER PRIME FIELDS

AMIT GHOSH AND KENNETH WARD

ABSTRACT. We consider canonical polynomial truncations of hypergeometric functions over the finite field $\mathbb{F}_p$, for primes $p \to \infty$. For these truncations, we obtain bounds for the number of roots of various modulo p congruences, which represent rational point counts where methods from classical algebraic geometry fail. Via a correspondence to families of elliptic curves, we obtain sharp bounds in some cases. We show that these truncations are also associated with certain surfaces, which we prove are K3. By a modification of methods from transcendence theory, we obtain a power saving for a large natural class of the parameter values within an algebraic closure of $\mathbb{F}_p$ for the Kummer hypergeometrics. Some computations are included to illustrate and supplement our results.

1. Introduction

In [GW15], we considered the following problem in modular arithmetic: Given a prime number $p > 3$ and a power series $F(x) = \sum_{n=0}^{\infty} a_n x^n$ with rational coefficients, suppose that there is an integer N as large as possible, but not exceeding $p-1$, such that the polynomial $F_N(x) = \sum_{n=0}^{N} a_n x^n$ is well-defined over the prime field $\mathbb{F}_p$. If N grows with p, then for any fixed m, what is the number of solutions to the congruence $F(x) \equiv m \pmod{p}$?

The reason for our consideration of this problem originally derived from the following failure of the Weil bound: for a polynomial f of degree d, the number of roots to the congruence $f \equiv m \pmod{p}$ is bounded by $d\sqrt{p}$, which is trivial if d exceeds $\sqrt{p}$. If $F(x)$ satisfies certain linear differential equations of order k with polynomial coefficients, then for $k = 1$, particularly for the truncations of the power series for the exponential and logarithm functions

$$E(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^{p-1}}{(p-1)!} \quad \text{and} \quad L(x) = x + \frac{x^2}{2} + \cdots + \frac{x^{p-1}}{p-1},$$

Mit'kin ($E(x)$ and $L(x)$) and independently, Heath-Brown ($L(x)$) showed that the number of roots in $\mathbb{F}_p$ is bounded by $O(p^{2/3})$ as $p \to \infty$. For each $k \geq 2$, examples of F are given in [GW15], for which the congruences have $o(p)$ solutions, for any given m, and in some cases a power saving is attained (see [GW15] for a more complete discussion and references).

In this paper, we explore this question by considering the hypergeometric functions and their truncations. In much of what follows, we shall consider hypergeometric functions with rational parameters, with the exception of Section 8 and Theorem 1.4 below, where it is natural to take parameter values in $\overline{\mathbb{F}}_p$ for the modular analogue to

classical transcendence theory. The bulk of the paper considers the functions ${}_2F_1$ and ${}_3F_2$ defined as follows: For $d \geq 2$,

$$ {}_dF_{d-1}\left(\alpha_1,\ldots,\alpha_d;\beta_1,\ldots,\beta_{d-1};x\right) = \sum_{n=0}^{\infty} \frac{(\alpha_1)_n \ldots (\alpha_d)_n}{n!(\beta_1)_n \ldots (\beta_{d-1})_n} x^n, \tag{1.0.1}$$

where $(a)_n = a(a+1)\cdots(a+n-1)$ is the Pochammer product. The Kummer hypergeometric function ${}_1F_1$ is defined similarly. We will evaluate these functions with parameter values arising from geometry: For the functions ${}_2F_1$ and ${}_3F_2$, these parameters give rise to non-cocompact arithmetic groups as the associated monodromy groups, and for ${}_1F_1$, the parameters will be precisely those analogous to *non-integers* over $\mathbb{F}_p$.

In the definition (1.0.1) of the hypergeometric function, if the α_i's and β_j's are rational numbers between zero and one, then there is a natural truncation of the given hypergeometric function F for any prime integer $p > 2$, which we will denote by $F^{(p)}$ (see Section 3 for details). These truncations are polynomials with degree N where $N \leq p-1$ and $\frac{N}{p} \sim r$ as p grows, with r a positive rational number that depends explicitly on the parameters of the hypergeometric function, via the residue classes of p modulo these parameters. A classical example is the Hasse polynomial $H_p(x)$, which is obtained by truncating ${}_2F_1\left(\frac{1}{2},\frac{1}{2};1;x\right)$ at $N = \frac{p-1}{2}$ for $p > 2$. It is known, for example, that the function $H_p(x)$ divides $x^{(p^2-1)/8}-1$, i.e., all roots of H are 8th powers of elements of $\mathbb{F}_{p^2}$, and that the number of roots of $H_p(x)$ in $\mathbb{F}_p$ is equal to precisely

$$N_p(H_p) = \begin{cases} 0, & \text{if } p \equiv 1 \mod 4 \\ 3h(-p), & \text{if } p \equiv 3 \mod 4, \end{cases}$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$ [BM04]. Since this example forms the basis of the geometric arguments which follow, we give a detailed explanation here.

Consider the Legendre family of elliptic curves $y^2 = x(x+1)(x+\lambda)$ over $\mathbb{F}_p$ with $\lambda \neq 0,-1 \pmod p$. For each curve in this family determined by a λ, we let $n_p(\lambda)$ denote the number of $\mathbb{F}_p$-rational points, so that $a_p(\lambda) := n_p(\lambda) - p - 1$ satisfies the Hasse estimate $|a_p(\lambda)| \leq 2\sqrt{p}$. It was shown by Igusa (as well as Manin and Dwork) that $a_p(\lambda) \equiv (-1)^{(p-1)/2}\ {}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{2};1,\lambda\right) \pmod p$. Thus, for a fixed integer m, the number of solutions to the polynomial congruence ${}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{2};1,\lambda\right) \equiv m \pmod p$ is the same as the number of $\mathbb{F}_p$-isomorphism classes of Legendre elliptic curves satisfying the condition $a_p(\lambda) \equiv (-1)^{(p-1)/2} m \pmod p$. The case $m = 0$ counts the number of supersingular such curves. The Hasse estimates imply that there exist no such λ if $|m| > 2\sqrt{p}$. On the other hand, if $|m| < 2\sqrt{p}$, Deuring [Deu41] showed that the number of such isomorphism classes for the family $y^2 = x^3 + ax + b$ with parameters a and b is essentially equal to the Hurwitz-Kronecker class number $H(m^2-4p)$ of an imaginary quadratic field (the classes counted up to a weight of $1/|\mathrm{Aut}(E)|$). From this we deduce an upper bound for the number of such isomorphism classes restricted to our 1-parameter family (see Section 7) so that the number of solutions to the congruence ${}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{2};1,\lambda\right) \equiv m \pmod p$ is $O\left(H(m^2-4p)\right)$. Then using Proposition 1.9 of Lenstra [Len87] we conclude that the number of roots in $\mathbb{F}_p$ of the congruence is at most $O\left(\sqrt{p}\log p(\log\log p)^2\right)$ for $|m| < 2\sqrt{p}$ and is zero otherwise. Since the m's are concentrated in a narrow range, it is clear that there are congruence classes m for which the root count exceeds $\varepsilon\sqrt{p}$ for p large enough, so that the upper bound is quite sharp.

The goal of this paper is a study of examples of truncated functions, arising naturally from geometry, for which one can obtain (sometimes sharp) bounds for the number of roots of the associated congruence. In Section 5, we consider three other families of elliptic curves apart from the Legendre family, which give rise to truncations of ${}_2F_1\left(\frac{a}{b}, 1-\frac{a}{b}; 1, \lambda\right)$ with $b = 3, 4$ and 6. Various classical transformation formulae are used in Section 4 to find analogous formulae over $\mathbb{F}_p$, which give relations between truncations of hypergeometric functions. The classical Clausen formula yields truncations of certain ${}_3F_2$ hypergeometrics, which are then associated to four families of K3 surfaces. We apply the same argument using Deuring's theorem to the three elliptic families to deduce, using the transformations formulae, bounds for the number of roots for congruences of the type $F(x) \equiv m \pmod{p}$. We note that due to the nature of the classical transformations, it is sometimes necessary to restrict the variables x to certain subsequences, and thus in some cases one may only conclude a bound for $m = 0$. We obtain non-trivial results for truncations of thirteen ${}_2F_1$ and four ${}_3F_2$ hypergeometric functions. The following Theorem and Corollary give these.

Theorem 1.1. *Let $\alpha \in \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{6}\}$ and put $\alpha = \frac{1}{b}$. Let Q denote any of the polynomials ${}_2F_1^{(p)}(\alpha, 1-\alpha; 1, x)$ and let X_p denote the quantity $\sqrt{p}\log p(\log\log p)^2$. Then for any m satisfying $|m| < 2\sqrt{p}$, the congruence $Q \equiv m \pmod{p}$ has $O\left(X_p\right)$ solutions for all p sufficiently large. Otherwise, the congruence has no solutions. Moreover, there are m's such that the corresponding congruences have more than $(\frac{1}{4} - \varepsilon)\sqrt{p}$ solutions for sufficiently small $\varepsilon > 0$.*

Corollary 1.2. *For α and p as above we have the following: :*

(I) Let Q denote the polynomials ${}_3F_2^{(p)}\left(\alpha, 1-\alpha, \frac{1}{2}; 1, 1, 4x(1-x)\right)$. Then the congruence $Q \equiv m \pmod{p}$ has $O\left(X_p\right)$ solutions for all m satisfying $m \equiv a^2 \pmod{p}$ with $|a| < 2\sqrt{p}$. Otherwise, the congruence has no solutions.

(II) Let Q be any of the polynomials ${}_2F_1^{(p)}(\alpha, \alpha; 1, x)$ and ${}_2F_1^{(p)}(1-\alpha, 1-\alpha; 1, x)$. Then, the congruence $Q \equiv 0 \pmod{p}$ has $O\left(X_p\right)$ solutions. If $m \neq 0$, the same conclusion holds for the congruence $Q \equiv m \pmod{p}$ for those large p satisfying $p \equiv 1 \pmod{b}$.

(III) Let $Q = {}_2F_1^{(p)}\left(\frac{\alpha}{2}, \frac{1}{2} - \frac{\alpha}{2}; 1, 4x(1-x)\right)$. If $p \equiv 1$ or $b-1 \pmod{2b}$, then the same conclusion holds for the congruence $Q \equiv m \pmod{p}$ as in the Theorem.

(IV) Let Q denote the polynomials ${}_2F_1^{(p)}\left(\alpha, \frac{1}{2}; 1, 1-x^2\right)$. If $p \equiv 1 \pmod{2b}$, then the congruence $Q \equiv m \pmod{p}$ has $O\left(X_p\right)$ solutions. For general p, the congruence $Q \equiv 0 \pmod{p}$ has at most the same number of solutions.

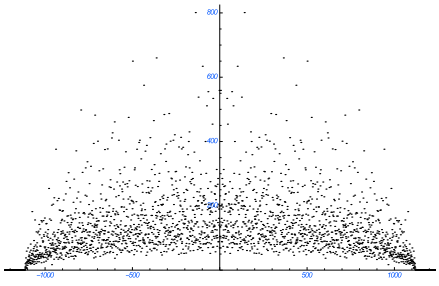
For all the cases there are m's such that the corresponding congruences have more than $\varepsilon\sqrt{p}$ solutions for sufficiently small $\varepsilon > 0$.

Remark 1.3. In [AOP02], a pairing of an elliptic family and a $K3$ family is considered to determine when elements of the $K3$ family are modular. A transformation formula was determined independently of the classical formulae. In the Appendix, we provide a separate proof of such a transformation formula over $\mathbb{F}_p$. The analysis in [AOP02] uses character sums, while our exposition for congruences is simpler, using binomial coefficients. A consequence is that the classical Clausen formula follows from that of the prime field case (see Remark 6.3). We expect that such equivalences are true for all of the formulae considered in Lemma 3.5.

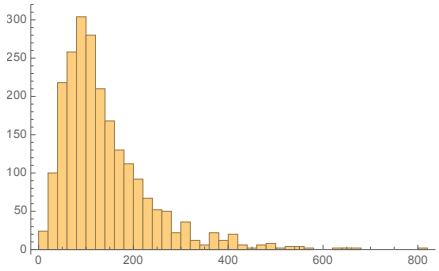
We give some sample plots for the distribution of $\mathcal{N}_p(m)$, the number of roots of $F \equiv_p m$ against m, with m in appropriate ranges. Our computations have p relatively

small due to the time it takes to complete them (as the degrees of the polynomials are quite large), primarily on a PC, and so we do not make any extravagant suggestions.

We see a rather singular behavior shown by Theorem 1.1 for the first four hypergeometric functions where the value distribution modulo p mimics the value distribution of the Hurwitz-Kronecker class numbers, as illustrated in Figs. 1 and 2. In Fig. 1 we plot $\mathscr{N}_p(m)$ against m together with the histogram for the distribution of $\mathscr{N}_p(m)$, whilst in Fig. 2 we plot $H(m^2-4p)$ against m and its histogram.

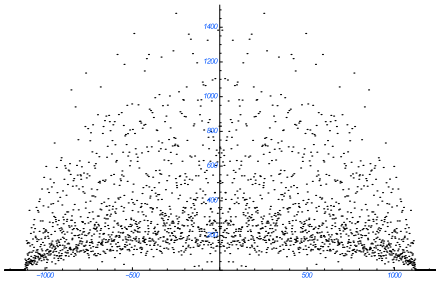


$F \equiv_p m,\ 0 \le |m| \le 2\sqrt{p}$

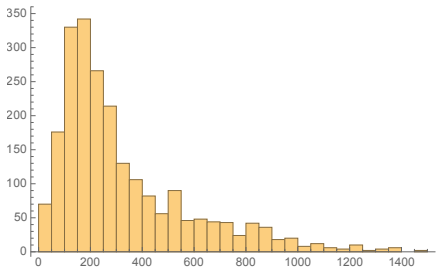


Histograms for value distribution.

FIGURE 1. ${}_2F_1^{(p)}\left(\frac{1}{6},\frac{5}{6},1;x\right);\quad p=312619$

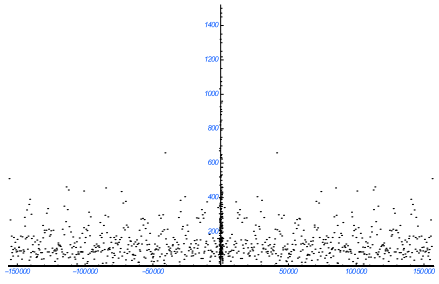


$H(m^2-4p),\ 0 \le |m| \le 2\sqrt{p}$

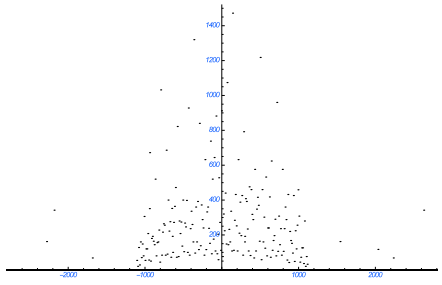


Histograms for value distribution.

FIGURE 2. Class number: $\quad p=312619$



$F \equiv_p m,\ 0 \le |m| \le \frac{p-1}{2}$



$-5\sqrt{p} \le m \le 5\sqrt{p}$

FIGURE 3. ${}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{3},1;1-x^2\right);\quad p=312619$

The monodromy groups associated with the ${}_2F_1$ hypergeometric functions appearing in Theorem 1.1 and the Corollary are equivalent to the nine non-cocompact arithmetic triangle groups (see [Tak77]). In Fig. 3, we see an example where the distribution is more spread out but with a concentration again in a short range.

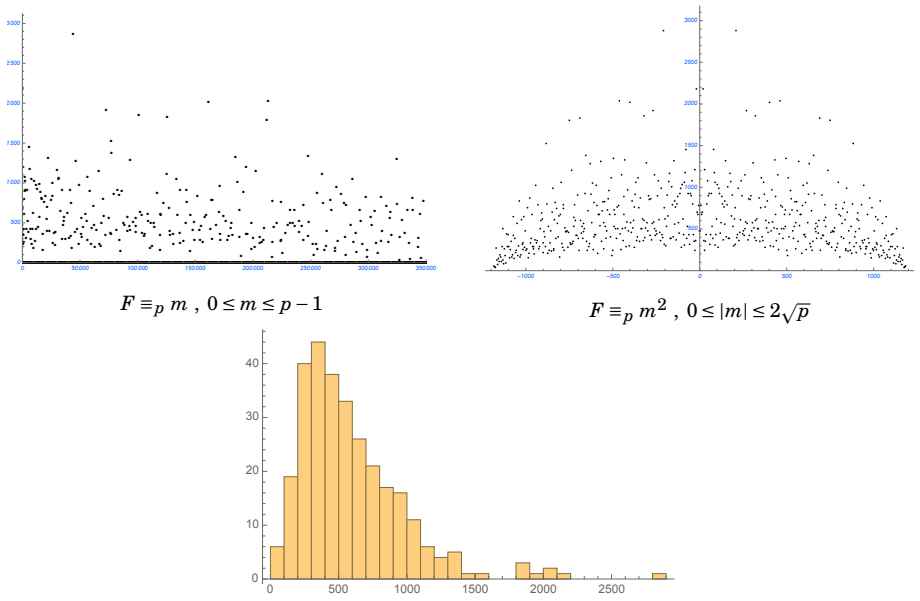
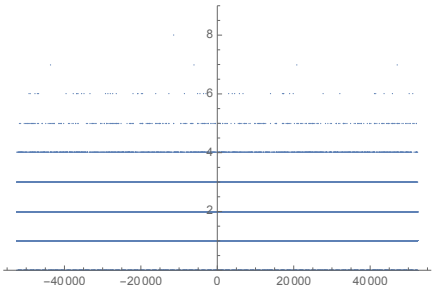


FIGURE 4. ${}_3F_2^{(p)}\left(\frac{1}{2},\frac{1}{2},\frac{1}{2};1,1;4x(1-x)\right)$; $p = 350381$.

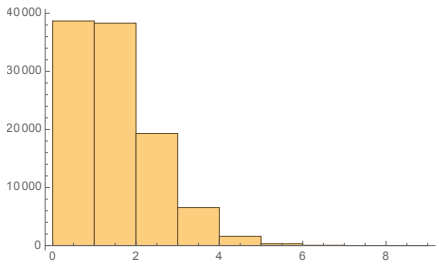
By [FMS14], there are six (orthogonal, quasiunipotent) arithmetic hypergeometric groups, of which four fix isotropic forms while two fix anisotropic forms (see the Table 2 and the Appendix of [FMS14]). The four ${}_3F_2$'s in Corollary 1.2 have monodromy groups equivalent to these four hypergeometric groups, and each have an associated fundamental domain that is non-compact. The value distribution of these truncated functions is illustrated in Fig. 4; computationally, we find that the value distribution of the truncated hypergeometric functions associated with the two anisotropic forms have a different behavior, akin to the pictures in Figs. 5 and 6 (the associated fundamental domains here are compact).

It appears that Fig. 5 represents the generic situation in many computations we have done. One might venture to guess, by looking at the graph in Fig. 5 that in these cases the maximum value for $\mathcal{N}_p(m)$ is bounded (independently of p), but we suspect that it is more likely growing but perhaps at a rate much slower than p^{ε} (for algebraic hypergeometrics, it might well be bounded). For instance, if one assumes the Poisson-like behavior for $\mathcal{N}_p(m)$ of Fig. 5, then one might expect that the maximum value for $\mathcal{N}_p(m)$ will have size about $\frac{\log p}{\log\log p}$.

We find this Poisson-like behavior for thirteen of the fourteen ${}_4F_3$ hypergeometrics associated with Calabi-Yau 3-folds listed in [SV14]; these fourteen have sympletic monodromy groups and half are thin ([BT14]) and the other half arithmetic ([SV14],



$F \equiv_p m,\ |m| \le \frac{p-1}{2}$



Histogram: Poisson mean 1

FIGURE 5. Compact monodromy: ${}_3F_2^{(p)}\left(\frac{1}{3},\frac{2}{3},\frac{1}{2};\frac{1}{6},\frac{5}{6};x\right)$, $p = 104773$

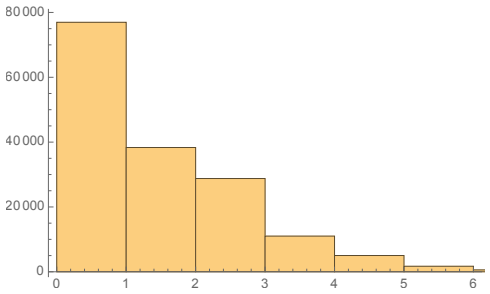


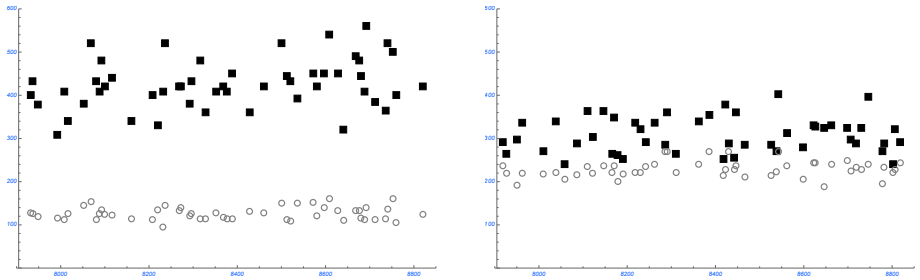
FIGURE 6. ${}_4F_3^{(p)}\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2};1,1,1;x\right)$, $p = 162601$

[Sin15]). The histograms for the associated $\mathcal{N}_p(m)$ all appear to be Poisson with mean 1 (as illustrated in Fig. 5), with the lone exception of ${}_4F_3^{(p)}\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2};1,1,1;x\right)$ whose histogram (Fig. 6) appears to be exponential in nature (so that we expect the maximal value for $\mathcal{N}_p(m)$ to be $\log p$ in this case).

In Figures 7 and 8, for $F = {}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{2},1;x\right)$, we let M_p denote the maximum value of $\mathcal{N}_p(m)$. Then, we let H_p denote the maximum of the Hurwitz-Kronecker class numbers $H(m^2-4p)$ over the same range of m's. The graphs denote a comparision of the plots of the points (p, M_p) and (p, H_p) as the primes p range over an interval. By Lemma 7.1, we know that $M_p \le 6H_p$, while the graphs show that perhaps more is true. In Figure 6, we plot the ratio M_p/H_p with p varying in the same range, but distinguishing the congruence classes modulo 4.

We now turn to hypergeometric functions for which the geometric method above is not available so that for these we use auxiliary polynomials as in transcendence theory (Stepanov's method). This approach(see [GW15] for example) has two distinct parts:

(1) the construction of auxiliary polynomials in many variables (of not too high degrees); and
(2) after specialisation, the non-vanishing of such polynomials, for which we need a form of algebraic independence of the truncated hypergeometrics and their derivatives over $\mathbb{F}_p$.



$p \equiv 1 \pmod 4$ $p \equiv 3 \pmod 4$

FIGURE 7. Maximal root counts (black) for ${}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{2},1;x\right)$ vs maximal class number (gray); primes $7919 \le p \le 8821$

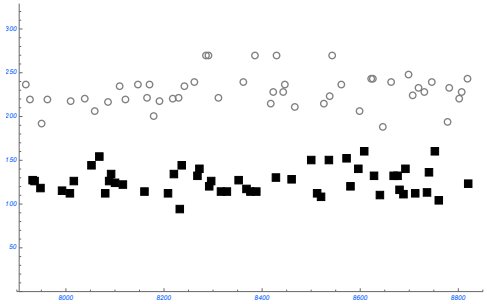


FIGURE 8. Ratio of maximal values relative to maximal class number (black: $p \equiv 1 \pmod 4$).

This latter problem is quite difficult, and the bounds obtained are not very sharp. However its advantage is it generality, and in some cases allows us to save a small power of p, as we obtained in [GW15] for the truncation of the Bessel function. In this vein, we show that a power saving is also possible for Kummer hypergeometric function ${}_1F_1\left(\alpha;\beta;z\right) = \sum_n^\infty \frac{(\alpha)_n}{(\beta)_n}\frac{z^n}{n!}$, for which we do not have an analog of the method using elliptic curves.

Theorem 1.4. *Let p be a sufficiently large prime number, let $\alpha \in \mathbb{F}_q$ ($q = p^m$) such that $\alpha \notin \mathbb{F}_p$, and let β be a fixed rational number. Then there is a bounded integer $k \ge 1$, determined by α, β and p, and an effectively computable constant $\kappa > 0$ such that the number of solutions in $\mathbb{F}_p$ to ${}_1F_1^{(p)}\left(\alpha;\beta;x^k\right) \equiv 0 \pmod p$ is $O(p^{1-\kappa})$. If instead $\beta \in \mathbb{F}_q$ and $\alpha, \alpha-\beta \notin \mathbb{F}_p$, then we may take $k = 1$.*

Example 1.4.1. Let α be a generator of $\mathbb{F}_q^*$ ($q = p^m, m \ge 2$) and $\beta = \frac{1}{3}$. Then ${}_1F_1^{(p)}\left(\alpha;\beta;x\right)$ has degree $\frac{p-1}{3}$ or $\frac{2p-1}{3}$ (depending on $p \equiv \pm 1 \pmod 6$) and we take $k = 3$.

Example 1.4.2. Let $\alpha, \beta \in \mathbb{F}_q$ such that the sets $\{\alpha + a \mid a \in \mathbb{F}_p\}$ and $\{\beta + a \mid a \in \mathbb{F}_p\}$ are disjoint. Then ${}_1F_1^{(p)}\left(\alpha;\beta;x\right)$ has degree $p-1$ and so we take $k = 1$.

The proof differs from that given for the Bessel function in [GW15], where an adaptation of methods from transcendence theory was used to count roots of the truncated

series. There the non-vanishing of the auxiliary polynomial for the Bessel function relied upon a modular version of the residue theorem, whereas here the argument for the Kummer hypergeometric relies upon a non-vanishing of certain coefficients of large degree *less than* p. We believe that these methods carry sufficiently general features that similar results are possible for other such hypergeometric functions.

Remark 1.5. The proof in Section 8 allows us to take $\kappa = \frac{1}{7}$. Unlike in Theorem 1.1, the element α (and β, if $\beta \in \mathbb{F}_q$) in Theorem 1.4 depend on p. The definition of the Pochhammer product in $\mathbb{F}_q$ is just the same as the usual one: If $a \in \mathbb{F}_q$, then

$$(a)_n = a(a+1)\cdots(a+n-1).$$

The notation $\equiv \pmod{p}$ in the statement of Theorem 1.4 is abusive, as the function ${}_1F_1^{(p)}\left(\alpha;\beta;x^k\right)$ is *a priori* reduced modulo p by taking $\alpha, \beta \in \mathbb{F}_q$. If $\alpha, \beta \in \mathbb{F}_q \setminus \mathbb{F}_p$, then the natural truncation occurs at $p-1$, and otherwise the truncation will have degree of the type $\frac{p-u}{v}$. In either case, ${}_1F_1^{(p)}\left(\alpha;\beta;x^k\right)$ will satisfy a differential equation with polynomial coefficients. If $v \neq 1$, there will be a coefficient whose degree will grow with p, which makes the construction of good auxiliary polynomials impossible. To overcome this, we impose the most natural change of variable to x^k, so that the resulting differential equation has coefficients with bounded degree.

Remark 1.6. As mentioned before, the algebraic independence over $\mathbb{F}_p$ is the difficult part of the proof. Our considerations rely on known proofs for the algebraic independence of functions and their derivatives over the complex numbers. This is a difficult problem in transcendence theory. There are some results known for Siegel E-functions due to Siegel [Sie49], Shidlovski [Shi11], Mahler [Mah76], Oleinikov [Ole68] and others. In characteristic $p > 0$, the derivative of x^p vanishes, and our argument relies upon an analysis of terms of highest degree less than p in the expression of a rational solution to the Riccati differential equation

$$y' + \frac{\beta - z}{z} y + y^2 \equiv \frac{\alpha}{z} \pmod{p}.$$

In Section 2, we make some observations about truncations of *rational* functions G, for which we see that the value distribution of a truncation $G^{(p)}$ is quite different from those of the polynomials we have considered above. There is usually a bounded number of roots in each congruence class, except possibly one class, which may account for almost all roots. The same kind of phenomenon is seen for algebraic hypergeometric functions (that is, all of those with finite monodromy group). This suggests that the value distribution modulo p of polynomials derived from algebraic power series is fundamentally different from those which are not algebraic.

Remark 1.7. In everything that follows, we use the notation $a \equiv_q b$ to mean the congruence $a \equiv b$ modulo q. We allow a and b to be rational numbers whose denominators are coprime to q.

Acknowledgments.
AG thanks Enrico Bombieri and Nick Katz for some conversations related to this work, and he thanks Peter Sarnak for some long discussions. He also thanks the Institute for Advanced Study (IAS) for their hospitality. He gratefully acknowledges financial

support from the IAS, the College of A&S and the Department of Mathematics of his home university, and the Simons Foundation for a Collaboration Grant.
KW thanks the NYU-ECNU Institute of Mathematical Sciences and the American University Mellon Research Fund for their financial support.
Computations were done using Mathematica©10.2 on a Linux PC, and also the Zorro High-Performance Computing System at American University.

2. Rational functions

Suppose that $F(x) = c\frac{A(x)}{B(x)}$ ($A, B \in \mathbb{Z}[x]$) is a nonzero rational function regular at $x = 0$, with the Maclaurin series expansion $\sum_{n=0}^{\infty} f_n x^n$, so that $f_n \in \mathbb{Q}$ for all n. Then for all primes p large enough, the coefficients f_n have denominators not divisible by p. Given such a function F, we consider only those p sufficiently large that $f_{p-k} \not\equiv_p 0$ for some bounded $k \geq 1$ (here and in what follows, "bounded" means, "bounded relative to p"). Let $S_{F,p}$ denote those $x \in \mathbb{F}_p$ such that $B(x) \equiv_p 0$ if $k = 1$, and if $k \geq 2$, we also include $x = 0$. Let $F_p(x) = \sum_{n=0}^{p-k} f_n x^n$, and put $F - F_p = x^{p-k+1} G_p(x)$. Then if

$$Q_p(x) := B(x)F_p(x) - A(x),$$

we have $Q_p(x) = -x^{p-k+1} G_p B(x)$, so that $Q_p(x)$ has a zero of order at least $p - k + 1$ at $x = 0$. We write $Q_p(x) = x^{p-k+1} Q_p^*(x)$ for a polynomial $Q_p^*(x)$ of bounded degree. It follows from this that

$$x^{k-1}(B(x)F_p(x) - A(x)) \equiv xQ_p^*(x) \mod (x^p - x),$$

so that $R_p(x) := x^{k-1}(B(x)F_p(x) - A(x)) - xQ_p^*(x)$ vanishes for all x modulo p.

Fix an integer m, and suppose that $F_p(x_0) \equiv_p m$ for some $x_0 \in \mathbb{Z} \bmod p$. Define

$$R_{p,m}(x) := x^{k-1}(B(x)m - A(x)) - xQ_p^*(x),$$

which is of bounded degree and has x_0 as a root modulo p. If $R_{p,m}(x)$ is not identically zero in $\mathbb{F}_p$, then since it is of bounded degree, it possesses only a bounded number of roots, so that there are also only a bounded number of distinct roots to the congruence $F_p(x_0) \equiv_p m$. On the other hand, if $R_{p,m}(x)$ vanishes identically modulo p, we will have

$$R_p(x) \equiv_p x^{k-1} B(x)(F_p(x) - m),$$

so that $F_p(x) \equiv_p m$ for all $x \notin S_{F,p}$. It is also clear that this latter equivalence can occur for at most one congruence class m modulo p.

Next, suppose that x_0 is a root of multiplicity l of the polynomial $F_p(x) - m$ modulo p such that l grows with p. From the above, we have by definition that

$$x^{k-1}B(x)(F_p(x) - m) + x^{k-1}(mB(x) - A(x)) = x^p Q_p^*(x),$$

so that differentiating l times with respect to x yields

$$\frac{d^l}{dx^l}\left(x^{k-1}B(x)(F_p(x) - m)\right) \equiv_p 0 \mod (F_p(x) - m),$$

in $\mathbb{F}_p$, due to the bounded degrees of the other polynomials. Hence $x_0^{k-1} B(x_0) \equiv_p 0$, so that $x_0 \in S_{F,p}$. We then have the following:

Proposition 2.1. *Let F be a rational function as above. For a fixed $k \geq 1$, let p be a sufficiently large prime such that $f_{p-k} \not\equiv_p 0$. Then the congruence*

$$F_p(x) \equiv_p m$$

has at most a bounded number of solutions for each m, with at most one possible exceptional value $m = m_0$. For the exceptional m_0 (if it exists), all except a bounded number of elements $x \in \mathbb{F}_p$ are solutions, upon which the congruence $F_p(x) \equiv_p m$ has no solutions, except for a bounded number of values of m.

If we put $F(x) = \frac{1}{1-x}$, so that for $k = 1$ we have $F_p(x) = \sum_{n=0}^{p-1} x^n$, it then is clear that the Proposition holds with the exceptional $m = 1$. There are cases where one can prove the analogue of Proposition 2.1 for truncations of algebraic power series.

Example 2.1.1. For $d \geq 2$, $v \geq 1$ and $1 \leq u \leq v$, consider the algebraic generalised hypergeometric functions

$$F(x) := {}_dF_{d-1}\left(\frac{u}{vd}, \frac{u+v}{vd}, \ldots, \frac{u+(d-1)v}{vd}; \frac{1}{d}, \frac{2}{d}, \ldots, \frac{d-1}{d}; x\right).$$

It is easily checked that the nth coefficient of the Taylor series about $x = 0$ is equal to

$$a(n) = \frac{1}{(dn)!} \prod_{j=0}^{dn-1} \left(\frac{u}{v} + j\right).$$

Let p be any prime number such that $p \equiv 1 \pmod{dv}$. Then for $0 \leq n \leq E$ with $E = \frac{p-1}{vd}u$, we have $a(n) \equiv_p (-1)^{dn}\binom{(p-1)\frac{u}{v}}{dn}$. Truncation of the hypergeometric function at E and denoting by $F^{(p)}(x)$ the resulting polynomial gives

$$F^{(p)}((-x)^d) \equiv_p \sum_{n=0}^{E} \binom{(p-1)\frac{u}{v}}{dn} x^{dn} = \sum_{\substack{n=0 \\ d|n}}^{dE} \binom{dE}{n} x^n \equiv_p \frac{1}{d} \sum_{g \in \Sigma(d)} (1+gx)^{dE},$$

where $\Sigma(d) = \{g : g^d \equiv_p 1\}$. For any m, suppose that there is a value x_0 such that $F^{(p)}(x_0^d) \equiv_p m$. It is then not difficult to show that there is a polynomial G, of degree v^d and with coefficients independent of x_0, such that $G(m) \equiv_p 0$. Thus, for all but a bounded number of congruence classes m, the congruence $F^{(p)}(x^d) \equiv_p m$ has no solutions. It also follows that there is a congruence class m_0 that has a positive proportion of roots.

For example, if $d = 2$, let u, v be coprime positive integers such that $0 < \frac{u}{v} \leq 1$, and consider the hypergeometric function ${}_2F_1(\frac{u}{2v}, \frac{u+v}{2v}, \frac{1}{2}; x)$. It is algebraic with a dihedral monodromy group. Then for primes p such that $p \equiv 1 \pmod{2v}$ and $E = \frac{p-1}{2v}u$, the truncated function ${}_2F_1^{(p)}(\frac{u}{2v}, \frac{u+v}{2v}, \frac{1}{2}; x)$ satisfies

$${}_2F_1^{(p)}\left(\frac{u}{2v}, \frac{u+v}{2v}, \frac{1}{2}; x^2\right) \equiv_p \frac{1}{2}\left[(1-x)^{2E} + (1+x)^{2E}\right]$$

Choosing, say, $u = 2$ and $v = 3$, we have $E = \frac{p-1}{3}$ with $p \equiv_3 1$, and it follows from the above that m is a root of the congruence $(4m^3 - 1)^3 - 27m^3 \equiv_p 0$. This equation has at most 7 distinct roots modulo p, so that for all except at most 7 congruence classes m modulo p, the equation ${}_2F_1^{(p)}\left(\frac{1}{3}, \frac{5}{6}, \frac{1}{2}; x^2\right) \equiv_p m$ has no solutions.

3. Preliminary lemmas and notation

Given any power series $\sum_m^\infty a_m x^m$, we wish to determine a natural truncation modulo prime integers p. For hypergeometric functions, there is such a truncation when the

parameters are rational numbers. We shall consider only hypergeometric functions of the type

$$ {}_dF_{d-1}(\alpha_1,\ldots,\alpha_d;\alpha_{i+1},\ldots,\alpha_{2d-1};x), \quad \alpha_i=\frac{a_i}{b_i}, \quad a_i,b_i\in\mathbb{N}, \quad (a_i,b_i)=1, \quad a_i\le b_i. $$

For any odd prime p sufficiently large so that p does not divide a_ib_i, for all i, we observe that $(\alpha_i)_m \equiv_p 0$ implies the same for all $n \ge m$. Thus for the numerator and denominator values α_i, we seek the largest $N \le p-1$ such that $(\alpha_i)_N$ is not divisible by p. This is equivalent to determining the smallest n_i such that $a_i + n_ib_i \equiv_p 0$. If $b_i = 1$, we take $n_i = p - a_i$. Otherwise, for $b_i > 1$, let u_i be the smallest positive residue of $a_i\overline{p}$ modulo b_i. Then the requisite n_i is given by $\frac{u_ip-a_i}{b_i}$ (note that $1 \le n_i \le p-1$). Therefore, the natural truncation must occur with $m \le N$ where $N = \min_i n_i$, the minimum of all of the values of n_i determined by all of the parameters. It follows that there exists a parameter $\frac{a}{b}$ and an integer $1 \le \omega \le b-1$, determined by the prime p, such that the natural truncation occurs at $N = \frac{\omega p-a}{b}$. In particular, we have that $\frac{N}{p}$ is asymptotically a positive rational number less than one. For the example ${}_2F_1\left(\frac{1}{3},\frac{5}{6},\frac{1}{2};x\right)$ considered in Section 2, if $p \equiv_6 1$, then the values of n are $\left\{\frac{p-1}{3},\frac{5(p-1)}{6},\frac{p-1}{2}\right\}$, so that $N=\frac{p-1}{3}$, but if on the other hand $p \equiv_6 5$, then the values of n are $\left\{\frac{2p-1}{3},\frac{p-5}{6},\frac{p-1}{2}\right\}$, so that now one must truncate at $N=\frac{p-5}{6}$.

In everything we consider henceforth, we will use this natural truncation. For a hypergeometric function F and a (sufficiently large) prime number p, we will denote the natural truncation by $F^{(p)}$, where the *degree* N as determined above is implicit.

We now state some results that will be used in later sections. Here and in what follows, p is any odd prime, and $D=\frac{p-1}{2}$.

Lemma 3.1. *Suppose that a and b are non-negative integers satisfying $0 \le a+b \le 2D$. Then*

$$ \binom{2D-a}{b} \equiv_p (-1)^b \binom{a+b}{a} \equiv_p (-1)^{a+b}\binom{2D-b}{a}. $$

Proof. This follows from the identities

$$ \binom{2D-a}{b} = \frac{1}{b!}\prod_{j=0}^{b-1}(2D-a-j) \equiv_p \frac{(-1)^b}{b!}\prod_{j=0}^{b-1}(1+a+j) = (-1)^b\binom{a+b}{b}. $$

□

Taking $a=0$, we obtain:

Corollary 3.2. *For each integer s with $0 \le s \le 2D$, we have*

$$ \binom{2D}{s} \equiv_p (-1)^s. $$

Corollary 3.3. *Suppose that $0 \le a \le D$. Then*

$$ \binom{2D-a}{a} \equiv_p 4^a\binom{D}{a}. $$

Proof. By Lemma 3.1, we have $\binom{2D-a}{a} \equiv_p (-1)^a \binom{2a}{a}$. Also, by definition, we have

$$\binom{D}{a} 2^a a! \equiv_p \prod_{j=0}^{a-1} (-1-2j) = (-1)^a \frac{(2a)!}{2^a (a!)}.$$

The result follows. □

If a and b are integers with $a, b \geq 0$, we define

$$S(a,b) := \sum_{x \in \mathbb{F}_p} x^a (1+x)^b. \tag{3.3.1}$$

The following characterisation of $S(a,b)$ will be important for rational point counts.

Lemma 3.4. *Suppose that a and b are integers with $a, b \geq 0$.*

(I) If $a > 0$ and if $2D \nmid b$, then

$$S(a,b) \equiv_p - \sum_{\substack{j=0 \\ 2D \mid a+j}}^{b} \binom{b}{j};$$

(II) If additionally $a + b < 4D$, then

$$S(a,b) \equiv_p -\binom{b}{2D-a}.$$

Proof. By definition, we have

$$S(a,b) = \sum_{j=0}^{b} \binom{b}{j} \sum_{x \in \mathbb{F}_p} x^{a+j}.$$

If α is a non-negative integer so that $2D \nmid \alpha$, then $\sum_{x \in \mathbb{F}_p} x^\alpha \equiv_p 0$. If on the other hand $2D \mid \alpha$ and $\alpha \geq 1$, then $\sum_{x \in \mathbb{F}_p} x^\alpha \equiv_p -1$. Also trivially if $\alpha = 0$, then $\sum_{x \in \mathbb{F}_p} x^\alpha \equiv_p 0$. As $2D \nmid a$, it follows that $a + j \geq 1$. This proves (i).

For (II), if $a + b < 4D$, then $2D \mid (a+j)$ in the sum implies that $a + j$ is equal to 0 or $2D$. The sum is zero at $j = 0$, so we only need consider the case $a + j = 2D$. The result then follows from the previous arguments. □

We state some classical transformation formulae for ${}_2F_1$ and ${}_3F_2$ hypergeometric functions as follows.

Lemma 3.5.

(I) Euler:

$${}_2F_1(a,b,c;x) = (1-x)^{c-a-b} \, {}_2F_1(c-a, c-b, c; x) \, .$$

(II) Pfaff:

$${}_2F_1(a,b,c;x) = (1-x)^{-a} \, {}_2F_1\left(a, c-b, c; \frac{-x}{1-x}\right).$$

(III) Quadratic:

(i)

$$\begin{aligned} {}_2F_1(a,1-a,c;x) &= (1-x)^{c-1} \, {}_2F_1\left(\frac{1}{2}a, \frac{1}{2} - \frac{1}{2}a, c; 4x(1-x)\right) \, , \\ &= (1-x)^{c-1}(1-2x)^{2c-1} \, {}_2F_1\left(c - \frac{1}{2}a, c - \frac{1}{2} + \frac{1}{2}a, c; 4x(1-x)\right) \, ; \end{aligned}$$

(ii)

$$ {}_2F_1(a,b,2b;x) = (1-x)^{-a/2}\ {}_2F_1\left(\frac{1}{2}a, b-\frac{1}{2}a, b+\frac{1}{2}; \frac{x^2}{4x-4}\right). $$

(IV) Clausen:

$$ {}_2F_1\left(a,b,a+b+\frac{1}{2};x\right)^2 = {}_3F_2\left(2a,2b,a+b;a+b+\frac{1}{2},2a+2b;x\right). $$

The natural $\mathbb{F}_p$ analogues of these formulae will be proven in Section 4.

4. Transformation formulae

4.1. Euler and Pfaff transformations

We consider here transformation formulae modulo p for truncations of hypergeometric functions of the form ${}_2F_1\left(\frac{a}{b},\frac{a}{b},1;x\right)$ and ${}_2F_1\left(\frac{a}{b},1-\frac{a}{b},1;x\right)$, where as before, $1 \le a < b$ with a and b coprime. We first determine the degrees of the truncations. Let $1 \le \omega \le b-1$ (see Section 3) satisfy $p\omega \equiv a$ modulo b, and let $E := \frac{\omega p - a}{b}$ denote the degree of ${}_2F_1^{(p)}\left(\frac{a}{b},\frac{a}{b},1;x\right)$. Then the corresponding ω' for ${}_2F_1^{(p)}\left(1-\frac{a}{b},1-\frac{a}{b},1;x\right)$ is $\omega' = b-\omega$, so that the degree of the truncation is equal to $2D-E$. Finally, for ${}_2F_1^{(p)}\left(\frac{a}{b},1-\frac{a}{b},1;x\right)$, the corresponding values of ω (resp. ω') are ω and $b-\omega$, so that the degree of the truncation is equal to $E^* := \min(E, 2D-E)$. We have the following:

Proposition 4.2. *Let $1 \le a < b$ be coprime integers. Then with E and E^* as above and for any (odd) prime $p > b$, we have:*
(I) If $E < \frac{p}{2}$ then

$$ {}_2F_1^{(p)}\left(\frac{a}{b},1-\frac{a}{b},1;x\right) \equiv_p\ (1-x)^{E^*}\ {}_2F_1^{(p)}\left(\frac{a}{b},\frac{a}{b},1;\frac{-x}{1-x}\right). $$

(II) If $E > \frac{p}{2}$ then

$$ {}_2F_1^{(p)}\left(\frac{a}{b},1-\frac{a}{b},1;x\right) \equiv_p\ (1-x)^{E^*}\ {}_2F_1^{(p)}\left(1-\frac{a}{b},1-\frac{a}{b},1;\frac{-x}{1-x}\right). $$

Proof. For the first case, $E^* = E$, and we use $m!\binom{E}{m} \equiv_p (-1)^m(\frac{a}{b})_m$. Then the right-hand side is congruent modulo p to

$$ \sum_n \binom{E}{n}^2 (-x)^n (1-x)^{E-n} = \sum_m \theta_m (-x)^m, $$

where

$$ \theta_m = \sum_l \binom{E-m+l}{l}\binom{E}{m-l}^2 = \binom{E}{m}\sum_l \binom{m}{l}\binom{E}{m-l} = \binom{E}{m}\binom{E+m}{m}. $$

Using $m!\binom{E+m}{m} \equiv_p (\frac{b-a}{b})_m$ then gives the result.

The proof of the second case is identical with $E^* = 2D-E$. □

We now consider the case of those b with $\phi(b) = 2$, so that $b = 3, 4$ or 6. Then $\frac{a}{b} = \frac{1}{b}$ or $1-\frac{1}{b}$. In the former case, $\omega = \overline{p}$, and in the latter, $\omega = b - \overline{p}$. Moreover, since $(p,b) = 1$, it follows that $p \equiv_b \pm 1$. Hence if $p \equiv_b 1$, then $E = \frac{p-1}{b} < \frac{p}{2}$ when $\frac{a}{b} = \frac{1}{b}$, so that we may apply Proposition 4.2(I). Similarly, if $p \equiv_b -1$, then $E = p - \frac{p+1}{b} > \frac{p}{2}$, so we apply Proposition 4.2(II) to obtain:

Corollary 4.3. *Let $b = 3,4$ or 6 and $p > b$, and let $K = \left\lfloor \frac{p-1}{b} \right\rfloor$. Then we have*
(I) If $p \equiv 1$ mod b, then

$$ {}_2F_1^{(p)}\left(\frac{1}{b}, 1-\frac{1}{b}, 1; x\right) \equiv_p (1-x)^K \; {}_2F_1^{(p)}\left(\frac{1}{b}, \frac{1}{b}, 1; \frac{-x}{1-x}\right) . $$

(II) If $p \equiv -1$ mod b, then

$$ {}_2F_1^{(p)}\left(\frac{1}{b}, 1-\frac{1}{b}, 1; x\right) \equiv_p (1-x)^K \; {}_2F_1^{(p)}\left(1-\frac{1}{b}, 1-\frac{1}{b}, 1; \frac{-x}{1-x}\right) . $$

The degree of the polynomials on both sides of each equation is equal to K.

The case of $\frac{a}{b} = 1 - \frac{1}{b}$ is of course identical to this.

Proposition 4.4. *Let $1 \le a < b$ be coprime integers. Then with E as above, for any odd prime p, we have*
(I) If $E < \frac{p}{2}$, then

$$ (1-x)^{2D-2E} \; {}_2F_1^{(p)}\left(\frac{a}{b}, \frac{a}{b}, 1; x\right) \equiv_p {}_2F_1^{(p)}\left(1-\frac{a}{b}, 1-\frac{a}{b}, 1; x\right) . $$

(II) If $E > \frac{p}{2}$, then

$$ {}_2F_1^{(p)}\left(\frac{a}{b}, \frac{a}{b}, 1; x\right) \equiv_p (1-x)^{2E-2D} \; {}_2F_1^{(p)}\left(1-\frac{a}{b}, 1-\frac{a}{b}, 1; x\right) . $$

Proof. For case (I), we again use $m!\binom{E}{m} \equiv_p (-1)^m (\frac{a}{b})_m$, so that

$$ {}_2F_1^{(p)}\left(\frac{a}{b}, \frac{a}{b}, 1; x\right) \equiv_p \sum_{m=0}^{E} \binom{E}{m}^2 x^m . $$

Expanding the left-hand side as a polynomial in x, we write it as $\sum_{m=0}^{2D-E} \alpha_m x^m$, where $\alpha_m = \sum_u (-1)^u \binom{2D-2E}{u} \binom{E}{m-u}^2$. Via

$$ \binom{2D-2E}{u}\binom{E}{m-u} = \binom{2D-E}{E}^{-1}\binom{2D-E}{m}\binom{2D-E-m}{2D-2E-u}\binom{m}{u}, $$

we write $\alpha_m = \binom{2D-E}{E}^{-1}\binom{2D-E}{m}\beta_m$, so that after the substitution $u \to m-u$, we obtain

$$ \beta_m = (-1)^m \sum_u (-1)^u \binom{m}{u}\binom{2D-E-m}{E-u}\binom{E}{u}. $$

The last two binomial coefficients in the expression above equal the coefficient of $x^{E-u}y^u$ in $(1+x)^{2D-E-m}(y+1)^E$. The substitution $y \to -x/t$ then yields equality to the coefficient of $x^E t^E$ in

$$ (-1)^u (1+x)^{2D-E-m} t^u [(1+t)-(1+x)]^E . $$

Summing over u shows that β_m is equal, up to multiplication by $(-1)^m$, to the coefficient of $x^E t^E$ in

$$ (1+x)^{2D-E-m}(1+t)^m [(1+t)-(1+x)]^E . $$

Expanding this expression yields

$$ \beta_m = (-1)^m \sum_s (-1)^s \binom{E}{s}\binom{E+m-s}{E}\binom{2D-E-m+s}{E}. $$

By Lemma 3.1, we have

$$\binom{2D-E-m+s}{E} = \binom{2D-(E+m-s)}{E} \equiv_p (-1)^{m-s}\binom{2D-E}{E+m-s}.$$

Thus

$$\binom{E}{s}\binom{E+m-s}{E}\binom{2D-E-m+s}{E} \equiv_p (-1)^{m-s}\binom{2D-E}{m}\binom{2D-E-m}{E-s}\binom{m}{s},$$

whence it follows that

$$\beta_m \equiv_p \binom{2D-E}{m}\sum_s \binom{2D-E-m}{E-s}\binom{m}{s} = \binom{2D-E}{m}\binom{2D-E}{E}.$$

Substituting this expression for β_m into α_m and using $m!\binom{2D-E}{m} \equiv_p (-1)^m(\frac{b-a}{b})_m$ yields the result.

For case (II), we replace $\frac{a}{b}$ in part (I) with $\frac{b-a}{b}$, which has the effect of replacing E with $2D-E < \frac{p}{2}$. Application of part (I) to the resulting expression gives the formula in (II), completing the proof. □

From this it follows:

Corollary 4.5. *Let $b = 3,4$ or 6, $p > b$, and $K = \left\lfloor \frac{p-1}{b} \right\rfloor$. Then we have*
(I) If $p \equiv 1$ mod b, then

$$(1-x)^{2D-2K}\ {}_2F_1^{(p)}\left(\frac{a}{b},\frac{a}{b},1;x\right) \equiv_p\ {}_2F_1^{(p)}\left(1-\frac{a}{b},1-\frac{a}{b},1;x\right).$$

(II) If $p \equiv -1$ mod b, then

$${}_2F_1^{(p)}\left(\frac{a}{b},\frac{a}{b},1;x\right) \equiv_p\ (1-x)^{2D-2K}\ {}_2F_1^{(p)}\left(1-\frac{a}{b},1-\frac{a}{b},1;x\right).$$

4.6. Clausen transformations

Consider the truncated hypergeometric function ${}_3F_2^{(p)}\left(\alpha,1-\alpha,\frac{1}{2};1,1;x\right)$, where $\alpha = \frac{a}{b}$ and $1 \le a < b$, with a and b coprime. We compute the degree of this truncation. Let $1 \le \Omega < b$ with $p\Omega \equiv_b a$, where $p > b$ is a prime number, and put $\hat{N} = \frac{p\Omega - a}{b}$. Since $1-\alpha = \frac{b-a}{b}$ with $(b-a,b) = 1$, the corresponding ω must satisfy $p\omega \equiv_b\ b-a$ with $0 < \omega < b$, so that $\omega = b - \Omega$. The corresponding N (see Section 3) is $2D - \hat{N}$ and the degree of the truncation is $N^* = \min\left(\hat{N}, 2D-\hat{N}, D\right)$.

It is easily checked that if $p > b$, then $\alpha = \frac{1}{2}$ if, and only if, $\hat{N} = D$ and $N^* = D$. Moreover, if $\alpha \ne \frac{1}{2}$, then $\hat{N} < D$ if, and only if, $2\Omega < b$. Thus, in this case, $N^* = \hat{N}$ if $2\Omega < b$, and $N^* = 2D - \hat{N}$ if $2\Omega > b$. We apply this to the values $b = 2,3,4$ and 6, those values of b with at most two reduced residue classes, to obtain:

Lemma 4.7.
Let N^* denote the degree of ${}_3F_2^{(p)}\left(\frac{1}{b},1-\frac{1}{b},\frac{1}{2};1,1;x\right)$, where $b = 2,3,4$ or 6. Then if $p > b$, we have

$$N^* = \begin{cases} \frac{p-1}{b}, & \text{if} \quad p \equiv_b\ 1 \\ \frac{p+1}{b} - 1, & \text{if} \quad p \equiv_b -1\,. \end{cases}$$

The degrees of ${}_2F_1^{(p)}\left(\frac{\alpha}{2},\frac{1}{2}-\frac{\alpha}{2};1;x\right)$ and ${}_2F_1^{(p)}\left(1-\frac{\alpha}{2},\frac{1}{2}+\frac{\alpha}{2};1;x\right)$ are computed next, with $\alpha = \frac{a}{b}$ as above.

4.7.1. For ${}_2F_1^{(p)}\left(\frac{\alpha}{2},\frac{1}{2}-\frac{\alpha}{2};1;x\right)$, we have several cases: (I) a even, b odd; (II) a and b both odd; and (III) a odd, b even.

(I) Put $a=2A$ and $b=B$ with B odd, so that $\frac{\alpha}{2}=\frac{A}{B}$ with $(A,B)=1$. Define $0<\omega<B$ such that $p\omega\equiv_B A$, and put $E=\frac{\omega p-A}{B}$. Then $\frac{1}{2}-\frac{\alpha}{2}=\frac{B-2A}{2B}$ with $(B-2A,2B)=1$. Thus the corresponding ω, denoted by ω', satisfies $p\omega'\equiv_{2B} B-2A$ with $0<\omega'<2B$. It follows that if $p>b$, then $\omega'=B-2\omega$ or $3B-2\omega$ depending on whether $\omega<\frac{B}{2}$ or $\omega>\frac{B}{2}$, respectively. The corresponding E (denoted by E') is then $D-E$ and $p-(E-D)$, respectively. It should be noted that if $p>b$, then $\omega<\frac{B}{2}$ if, and only if, $E<D$. By definition, the degree N^* of ${}_2F_1^{(p)}\left(\frac{\alpha}{2},\frac{1}{2}-\frac{\alpha}{2};1;x\right)$ is equal to $\min(E,E')$, so that we have:

(i) If $\omega<\frac{B}{2}$, then

$$N^*=\begin{cases}E, & \text{if } E\le\frac{1}{2}D\\ D-E, & \text{if } \frac{1}{2}D\le E<D\ .\end{cases}$$

(ii) If $\omega>\frac{B}{2}$, then

$$N^*=\begin{cases}E, & \text{if } D<E\le\frac{1}{2}(p+D)\\ p+D-E, & \text{if } E\ge\frac{1}{2}(p+D)\ .\end{cases}$$

When $b=2,3,4$ or 6, this case occurs only when $a=2$ and $b=3$. Then if N^* is the degree of ${}_2F_1^{(p)}\left(\frac{1}{3},\frac{1}{6};1;x\right)$, we have for $p>3$:

$$N^*=\begin{cases}\frac{1}{3}(p-1), & \text{if } p\equiv_6 1\\ \frac{1}{3}(2p-1), & \text{if } p\equiv_6 5\ .\end{cases}\tag{4.7.1}$$

(II) Since a and b are both odd and the hypergeometric is unchanged if a is replaced with $b-a$, we have the case above, so that N^* is the same.

(III) If a is odd and b is even, then ω satisfies $p\omega\equiv_{2b} a$, with $1\le\omega<2b$ and $E=\frac{\omega p-a}{2b}$. Since $(b-a,2b)=1$, it follows that $0<\omega'<2b$, with $p\omega\equiv_{2b} b-a$ and $E'=\frac{\omega' p-(b-a)}{2b}$. It then follows that $\omega'=b-\omega$ if $\omega<b$ and $\omega'=3b-\omega$ if $\omega>b$. The corresponding E' are then $E'=D-E$ and $E'=p-(E-D)$, respectively (as in the previous cases). For the choices of b as in Proposition 4.7, we then have $b=2,4$ or 6, so that

(i) If $b=2$, $a=1$, then for $p\ge3$

$$N^*=\begin{cases}\frac{1}{4}(p-1), & \text{if } p\equiv_4 1\\ \frac{1}{4}(3p-5), & \text{if } p\equiv_4 3\ .\end{cases}$$

(ii) If $b=4$, $a=1$ or 3, then for $p\ge5$

$$N^*=\begin{cases}\frac{1}{8}(p-1), & \text{if } p\equiv_8 1\\ \frac{1}{8}(p-3), & \text{if } p\equiv_8 3\\ \frac{1}{8}(5p-1), & \text{if } p\equiv_8 5\\ \frac{1}{8}(5p-3), & \text{if } p\equiv_8 7\ .\end{cases}$$

(iii) If $b=6$, $a=1$ or 5, then for $p\geq 7$

$$N^*=\begin{cases}\frac{1}{12}(p-1), & \text{if} \quad p\equiv_{12} 1\\ \frac{1}{12}(p-5), & \text{if} \quad p\equiv_{12} 5\\ \frac{1}{12}(7p-1), & \text{if} \quad p\equiv_{12} 7\\ \frac{1}{12}(7p-5), & \text{if} \quad p\equiv_{12} 11\,.\end{cases}$$

4.7.2. For ${}_2F_1^{(p)}\left(1-\frac{a}{2b},\frac{1}{2}+\frac{a}{2b};1;x\right)$ the analysis is similar:

(I) If a is even and b is odd, we write $1-\frac{a}{2b}=\frac{A}{B}$ and $\frac{1}{2}+\frac{a}{2b}=\frac{3B-2A}{2B}$, with B odd and all corresponding numerators and denominators coprime. Then we have $0<\omega<B$ satisfying $p\omega\equiv_B A$ and $E=\frac{p\omega-A}{B}$, and $0<\omega'<2B$ satisfying $p\omega\equiv_{2B} 3B-2A$ and $E'=\frac{p\omega'-(3B-2A)}{2B}$. It follows that $B|(2\omega+\omega')$, and since ω' is odd, that necessarily $\omega'=B-2\omega$ if $\omega<\frac{B}{2}$ or $\omega'=3B-2\omega$ otherwise. Hence $E'=D-1-E$ or $E'=p+D-1-E$ in the two instances, respectively (note that if $p>b$, then $E<D$ if, and only if, $\omega<\frac{B}{2}$). We thus have

(i) If $\omega<\frac{B}{2}$, then

$$N^*=\begin{cases}E, & \text{if} \quad E\leq\frac{1}{2}(D-1)\\ D-1-E, & \text{if} \quad \frac{1}{2}(D-1)\leq E<D\,.\end{cases}$$

(ii) If $\omega>\frac{B}{2}$, then

$$N^*=\begin{cases}E, & \text{if} \quad D<E\leq\frac{3}{2}D\\ p+D-1-E, & \text{if} \quad E\geq\frac{3}{2}D\,.\end{cases}$$

Applying this to the case $b=3$ and $a=2$, gives for $p>3$ that

$$N^*=\begin{cases}\frac{2}{3}(p-1), & \text{if} \quad p\equiv_6 1\\ \frac{1}{6}(p-5), & \text{if} \quad p\equiv_6 5\,.\end{cases} \tag{4.7.2}$$

(II) If a and b are both odd, (so that when $b=3$, $a=1$), the result is the same as in case (I) above.

(III) If a is odd and b is even, we write $1-\frac{a}{2b}=\frac{A}{B}$ with $A=2b-a$ and $B=2b$, so that $(A,B)=1$. We also write $\frac{1}{2}+\frac{a}{2b}=\frac{U}{V}$ with $U=\frac{3}{2}B-A$ and $V=B$, so that $(U,V)=1$. Then $0<\omega<B$ with $p\omega\equiv_B A$ and $E=\frac{\omega p-A}{B}$. Also, ω' $(0<\omega'<B)$ satisfies $p\omega'\equiv_B \frac{3}{2}B-A$. It follows that $B|2(\omega+\omega')$, so that if $p>b$, we have $\omega'=\frac{1}{2}B-\omega$ if $\omega<\frac{1}{2}B$, and $\omega'=\frac{3}{2}B-\omega$ otherwise. Hence $E'=D-E$ or $E'=p+D-E$. We then have the cases

(i) If $b=2$, $a=1$, then for $p\geq 3$,

$$N^*=\begin{cases}\frac{1}{4}(3p+1), & \text{if} \quad p\equiv_4 1\\ \frac{1}{4}(p-3), & \text{if} \quad p\equiv_4 3\,.\end{cases}$$

(ii) If $b=4$, $a=1$ or 3, then for $p\geq 5$

$$N^*=\begin{cases}\frac{1}{8}(5p+3), & \text{if} \quad p\equiv_8 1\\ \frac{1}{8}(5p-7), & \text{if} \quad p\equiv_8 3\\ \frac{1}{8}(p-5), & \text{if} \quad p\equiv_8 5\\ \frac{1}{8}(p-7), & \text{if} \quad p\equiv_8 7\,.\end{cases}$$

(iii) If $b = 6$, $a = 1$ or 5, then for $p \geq 7$

$$N^* = \begin{cases} \frac{1}{12}(7p+5), & \text{if} \quad p \equiv_{12} 1 \\ \frac{1}{12}(7p-11), & \text{if} \quad p \equiv_{12} 5 \\ \frac{1}{12}(p-7), & \text{if} \quad p \equiv_{12} 7 \\ \frac{1}{12}(p-11), & \text{if} \quad p \equiv_{12} 11\,. \end{cases}$$

Proposition 4.8. *Let $1 \leq a < b$ be coprime integers with $b = 3$, 4 or 6 as above. For any odd prime $p > b$*

$${}_3F_2^{(p)}\left(\frac{a}{b}, 1-\frac{a}{b}, \frac{1}{2}; 1, 1; x\right) \equiv_p \begin{cases} {}_2F_1^{(p)}\left(\frac{a}{2b}, \frac{1}{2}-\frac{a}{2b}; 1; x\right)^2, & \text{if} \quad p \equiv_{2b} 1,\ b-1 \\ (1-x)\ {}_2F_1^{(p)}\left(1-\frac{a}{2b}, \frac{1}{2}+\frac{a}{2b}; 1; x\right)^2, & \text{otherwise}\,; \end{cases}$$

where for $b = 3$ one discards the congruence class $p \equiv_6 2$.

Proof. The polynomials on both sides of the equations have the same degree modulo p. The results follow from an application of the classical transformation formulae. We provide the details for the first case, as the proof is the same as that for all of the other cases.

First, if $p \equiv_4 1$, then the degree of the ${}_3F_2^{(p)}$ in question is equal to D, while that of the ${}_2F_1^{(p)}$ is equal to $E = \frac{D}{2}$. Thus, comparing coefficients, we need to show that for $0 \leq m \leq D$,

$$\left(\frac{\left(\frac{1}{2}\right)_m}{m!}\right)^3 \equiv_p \sum_{\substack{0 \leq u,v, \leq E \\ u+v=m}} \left(\frac{\left(\frac{1}{4}\right)_u \left(\frac{1}{4}\right)_v}{u!v!}\right)^2. \tag{4.8.1}$$

However, by the definition of *degree*, the Pochhammer symbols on the right vanish modulo p if u or v exceed E. We may then remove the restrictions on u and v entirely (provided that $m \leq D$), so that (4.8.1) holds with equality using Clausen's formula in Lemma 3.5.

For $p \equiv_4 3$, the degree of the ${}_3F_2^{(p)}$ is equal to D, while the degree of the ${}_2F_1^{(p)}$ is equal to $E = \frac{p-3}{4}$. The proof by considering coefficients follows in exactly the same manner as above, by instead using a combination of Euler's and Clausen's formula as in Lemma 3.5 of the form

$${}_3F_2\left(2a, 2b, a+b; a+b+\frac{1}{2}, 2a+2b;\ x\right) = (1-x)\ {}_2F_1\left(a+\frac{1}{2}, b+\frac{1}{2}, a+b+\frac{1}{2};\ x\right)^2.$$

□

4.9. Quadratic transformations

We now turn to identities which relate these formulae to elliptic curves and K3 surfaces.

Proposition 4.10.

Let $1 \leq a < b$ be coprime integers with $b = 3$, 4 or 6 as above. For any odd prime $p > b$ we have

$${}_2F_1^{(p)}\left(\frac{a}{b}, \frac{b-a}{b}, 1; x\right) \equiv_p \begin{cases} {}_2F_1^{(p)}\left(\frac{a}{2b}, \frac{1}{2}-\frac{a}{2b}, 1;\ 4x(1-x)\right), & p \equiv_{2b} 1,\ b-1 \\ (1-2x)\ {}_2F_1^{(p)}\left(1-\frac{a}{2b}, \frac{1}{2}+\frac{a}{2b}, 1;\ 4x(1-x)\right), & \text{otherwise}\,; \end{cases}$$

where for $b = 3$ one discards the congruence class $p \equiv_6 2$.

Proof. Since $\phi(b)=2$, we may choose $a=1$, as all of the formulae are symmetric with $a \to b-a$. For b even, the degree of ${}_2F_1^{(p)}\left(\frac{1}{b}, 1-\frac{1}{b}, 1; x\right)$ is equal to $E^* = \frac{p-1}{b}$ or $\frac{p-(b-1)}{b}$, depending on the two congruence classes $p \equiv_b \pm 1$ respectively. It is then easily checked that the degree of ${}_2F_1^{(p)}\left(\frac{1}{2b}, \frac{1}{2}-\frac{1}{2b}, 1;\ x\right)$ is equal to $\frac{1}{2}E^*$ for the two congruence classes $p \equiv_{2b} 1$ or $b-1$. Similarly, one sees that the degree of ${}_2F_1^{(p)}\left(1-\frac{1}{2b}, \frac{1}{2}+\frac{1}{2b}, 1;\ x\right)$ is equal to $\frac{1}{2}(E^*-1)$ for the other two cases. Thus both sides of the equations have precisely the same degrees. The result now follows by using the classical quadratic transformations as in Lemma 3.5 and comparing coefficients in exactly the same manner as described above.

The case $b=3$ is similar. □

Lemma 4.11. *Let $b=3,\ 4$ or 6. Suppose E^* denotes the degree of ${}_2F_1^{(p)}\left(\frac{1}{2}, \frac{1}{b}, 1; x\right)$, N^* the degree of ${}_2F_1^{(p)}\left(\frac{1}{2b}, \frac{1}{2}-\frac{1}{2b}, 1; x\right)$ and N^{**} the degree of ${}_2F_1^{(p)}\left(\frac{1}{2}+\frac{1}{2b}, 1-\frac{1}{2b}, 1; x\right)$.*

(I) If $p \equiv_{2b} 1$ or $p \equiv_{2b} b-1$, then the values of E^* and N^* are as follows:

(a) If $b=3$, then for $p>3$, $(E^*, N^*) = \left(\frac{1}{3}(p-1), \frac{1}{6}(p-1)\right)$, if $p \equiv_6 1$.

(b) If $b=4$, then for $p \geq 5$,

$$(E^*, N^*) = \begin{cases} \left(\frac{1}{4}(p-1), \frac{1}{8}(p-1)\right), & \text{if } p \equiv_8 1 \\ \left(\frac{1}{2}(p-1), \frac{1}{8}(p-3)\right), & \text{if } p \equiv_8 3. \end{cases}$$

(c) If $b=6$, then for $p \geq 7$,

$$(E^*, N^*) = \begin{cases} \left(\frac{1}{6}(p-1), \frac{1}{12}(p-1)\right), & \text{if } p \equiv_{12} 1 \\ \left(\frac{1}{2}(p-1), \frac{1}{12}(p-5)\right), & \text{if } p \equiv_{12} 5. \end{cases}$$

(II) If $p \equiv_{2b} b+1$ or $p \equiv_{2b} 2b-1$, then the values of E^* and N^{**} are as follows:

(a) If $b=3$, then for $p>3$, $(E^*, N^{**}) = \left(\frac{1}{2}(p-1), \frac{1}{6}(p-5)\right)$ if $p \equiv_6 5$.

(b) If $b=4$, then for $p \geq 5$,

$$(E^*, N^{**}) = \begin{cases} \left(\frac{1}{4}(p-1), \frac{1}{8}(p-5)\right), & \text{if } p \equiv_8 5 \\ \left(\frac{1}{2}(p-1), \frac{1}{8}(p-7)\right), & \text{if } p \equiv_8 7. \end{cases}$$

(c) If $b=6$, then for $p \geq 7$,

$$(E^*, N^{**}) = \begin{cases} \left(\frac{1}{6}(p-1), \frac{1}{12}(p-7)\right), & \text{if } p \equiv_{12} 7 \\ \left(\frac{1}{2}(p-1), \frac{1}{12}(p-11)\right), & \text{if } p \equiv_{12} 11. \end{cases}$$

Proof. (I) Let E', N', and N'' denote the natural truncations associated with $(\frac{1}{b})_n$, $(\frac{1}{2b})_n$, and $(\frac{1}{2}-\frac{1}{2b})_n$ respectively, then by definition (see Section 3) we find that

(a) If $b=3$, then for $p>3$, $(E', E^*, N', N'', N^*) = (\frac{p-1}{3}, \frac{p-1}{3}, \frac{p-1}{6}, \frac{p-1}{3}, \frac{p-1}{6})$ if $p \equiv_6 1$.

(b) If $b=4$, then for $p \geq 5$,

$$(E', E^*, N', N'', N^*) = \begin{cases} (\frac{p-1}{4}, \frac{p-1}{4}, \frac{p-1}{8}, \frac{3(p-1)}{8}, \frac{p-1}{8}), & \text{if } p \equiv_8 1 \\ (\frac{3p-1}{4}, \frac{p-1}{2}, \frac{3p-1}{8}, \frac{p-3}{8}, \frac{p-3}{8}), & \text{if } p \equiv_8 3. \end{cases}$$

(c) If $b=6$, then for $p \geq 7$,

$$(E', E^*, N', N'', N^*) = \begin{cases} (\frac{p-1}{6}, \frac{p-1}{6}, \frac{p-1}{12}, \frac{5(p-1)}{12}, \frac{p-1}{12}), & \text{if } p \equiv_{12} 1 \\ (\frac{5p-1}{6}, \frac{p-1}{2}, \frac{5p-1}{12}, \frac{p-5}{12}, \frac{p-5}{12}), & \text{if } p \equiv_{12} 5. \end{cases}$$

The claim then follows from the definition of truncation.

The cases in (II) are obtained by a similar argument. □

Proposition 4.12. *Let $b=3,\ 4$ or 6. For any odd prime $p>b$ we have:*

(I) If

$$K = \begin{cases} \frac{p-1}{2b} & \text{if } p \equiv_{2b} 1 \\ \frac{(b-1)p-1}{2b} & \text{if } p \equiv_{2b} b-1, \end{cases}$$

then

$${}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{b},1;x\right) \equiv_p (1-x)^K {}_2F_1^{(p)}\left(\frac{1}{2b},\frac{1}{2}-\frac{1}{2b},1;\frac{x^2}{4x-4}\right).$$

(II) If

$$K = \begin{cases} \frac{p-(b+1)}{2b} & \text{if } p \equiv_{2b} b+1 \\ \frac{(b-1)p-(b+1)}{2b} & \text{if } p \equiv_{2b} 2b-1, \end{cases}$$

then

$${}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{b},1;x\right) \equiv_p \frac{1}{2}(2-x)(1-x)^K {}_2F_1^{(p)}\left(\frac{1}{2}+\frac{1}{2b},1-\frac{1}{2b},1;\frac{x^2}{4x-4}\right).$$

Proof. In characteristic zero, by Lemma 3.5(III)(ii) (a quadratic identity) with $a = \frac{1}{b}$ we have

$${}_2F_1\left(\frac{1}{b},\frac{1}{2},1;x\right) = (1-x)^{-\frac{1}{2b}} {}_2F_1\left(\frac{1}{2b},\frac{1}{2}-\frac{1}{2b},1;\frac{x^2}{4x-4}\right).$$

Then, by Lemma 3.5(I) (Euler's identity), we have

$$\begin{aligned} {}_2F_1\left(\frac{1}{2b},\frac{1}{2}-\frac{1}{2b},1;\frac{x^2}{4x-4}\right) &= \left(1-\frac{x^2}{4x-4}\right)^{\frac{1}{2}} {}_2F_1\left(1-\frac{1}{2b},\frac{1}{2}+\frac{1}{2b},1;\frac{x^2}{4x-4}\right), \\ &= \frac{1}{2}\left(\frac{(x-2)^2}{1-x}\right)^{\frac{1}{2}} {}_2F_1\left(1-\frac{1}{2b},\frac{1}{2}+\frac{1}{2b},1;\frac{x^2}{4x-4}\right), \\ &= \frac{1}{2}(1-x)^{-\frac{1}{2}}(2-x)\, {}_2F_1\left(1-\frac{1}{2b},\frac{1}{2}+\frac{1}{2b},1;\frac{x^2}{4x-4}\right), \end{aligned}$$

where the last equality follows as ${}_2F_1(\cdot,\cdot,\cdot;0) = 1$. Combining the above two formulae gives us

$$(4.12.1) \qquad {}_2F_1\left(\frac{1}{b},\frac{1}{2},1;x\right) = \frac{1}{2}(1-x)^{-\frac{1}{2}-\frac{1}{2b}}\,(2-x)\, {}_2F_1\left(1-\frac{1}{2b},\frac{1}{2}+\frac{1}{2b},1;\frac{x^2}{4x-4}\right).$$

We first prove case (II). By Lemma 4.11, if $p \equiv_{2b} b+1$, then

$$E^* = \frac{p-1}{b} \qquad \text{and} \qquad N^{**} = \frac{p-(b+1)}{2b},$$

and if $p \equiv_{2b} 2b-1$, then

$$E^* = \frac{p-1}{2} \qquad \text{and} \qquad N^{**} = \frac{p-(2b-1)}{2b}.$$

To ensure that the degrees of both sides of our identities are equal and that any denominators containing powers of $4x-4$ are removed, we require that $K \geq N^{**}$ and $E^* = K+1+N^{**}$, so that we need $E^* \geq 2N^{**}+1$. By Lemma 4.11, we have that if $p \equiv_{2b} b+1$, then

$$N^{**} = \frac{p-(b+1)}{2b} = \frac{p-1}{b} - \frac{p-(b+1)}{2b} - 1 \;=\; K,$$

and if $p \equiv_{2b} 2b-1$, then

$$N^{**} = \frac{p-(2b-1)}{2b} < \frac{(b-1)p-(b+1)}{2b} = \frac{p-1}{2} - \frac{p-(2b-1)}{2b} - 1 = K.$$

We write ${}_2F_1\left(\frac{1}{2}+\frac{1}{2b},1-\frac{1}{2b},1;x\right)=\sum_n \beta_n x^n$. With this notation,

$$\begin{aligned}\frac{1}{2}(2-x)(1-x)^K\ {}_2F_1^{(p)}\left(\frac{1}{2}+\frac{1}{2b},1-\frac{1}{2b},1;\frac{x^2}{4x-4}\right)&\\ =\frac{1}{2}(2-x)\sum_{n\le N^{**}}\beta_n x^{2n}\left(\frac{-1}{4}\right)^n(1-x)^{K-n},&\\ =\frac{1}{2}\sum_{n\le N^{**}}\beta_n x^{2n}\left(\frac{-1}{4}\right)^n\left[(1-x)^{K+1-n}+(1-x)^{K-n}\right],&\\ =\frac{1}{2}\sum_{n\le N^{**}}\sum_{j\ge 0}\beta_n\left(\frac{-1}{4}\right)^n\left[\binom{K+1-n}{j}+\binom{K-n}{j}\right]x^{2n+j}.&\end{aligned}$$

Putting $m=j+2n$; using the fact that necessarily $j\le K+1$ and using $E^*=K+1+N^{**}$, we see that $0\le m\le E^*$. Hence, the sum above is

$$\frac{1}{2}\sum_{0\le m\le E^*}x^m\left(\sum_{\substack{n\le N^{**},\,j\ge 0\\ j+2n=m}}\beta_n\left(\frac{-1}{4}\right)^n\left\{\binom{K+1-n}{j}+\binom{K-n}{j}\right\}\right).$$

For m in this range, the β_n's vanish (modulo p) if $n>N^{**}$, so that we may drop the restriction on n. Next, by elementary considerations, if $0\le j\le p-1$ and $p\equiv_{2b}\ b+1$, then for $s\in\mathbb{Z}$

$$\binom{K+s}{j}=\binom{\frac{p-(b+1)}{2b}+s}{j}\equiv_p\ \binom{\frac{-(b+1)}{2b}+s}{j}=\binom{-\frac{1}{2}-\frac{1}{2b}+s}{j};$$

and if $p\equiv_{2b}\ 2b-1$, then also

$$\binom{K+s}{j}=\binom{\frac{(b-1)p-(b+1)}{2b}+s}{j}\equiv_p\ \binom{\frac{-(b+1)}{2b}+s}{j}=\binom{-\frac{1}{2}-\frac{1}{2b}+s}{j}.$$

Moreover since $j\le m<p$, we see that there are no restrictions on j beyond that imposed by $m=2n+j$. It follows that the coefficient of x^m in the previous sum is equal modulo p to the respective coefficient in characteristic zero, whence the identity then follows from the classical case in (4.12.1).

In case (I), we have if either $p\equiv_{2b}1$ or $p\equiv_{2b}b-1$ that $K=N^*$. The argument then follows as in case (II), where it is only necessary to consider the coefficient $\binom{K-n}{j}\equiv_p\ \binom{-\frac{1}{2b}-n}{j}$. □

5. Elliptic families

Those ${}_2F_1(a,b,c;z)$ hypergeometric functions with integer coefficients and $c=1$ take the form ${}_2F_1(a,1-a,c;z)$, where $a=\frac{1}{2},\frac{1}{3},\frac{1}{4}$, or $\frac{1}{6}$. We now determine the families of elliptic curves associated with the mod p truncations of these functions.

(I) If $b = 2$, we have

$$\begin{aligned}
{}_2F_1^{(p)}\left(\frac{1}{2},\frac{1}{2};1;\lambda\right) &= \sum_{n=0}^{D}\frac{\left(\frac{1}{2}\right)_n^2}{(n!)^2}\lambda^n \\
&\equiv_p \sum_{n=0}^{D}\binom{D}{n}^2\lambda^n \\
&\equiv_p -\sum_{n=0}^{D}\binom{D}{n}\sum_{x\in\mathbb{F}_p}x^{2D-n}(x+1)^D\lambda^n \\
&\equiv_p \sum_{x\in\mathbb{F}_p}\left[x(x+1)(x+\lambda)\right]^D.
\end{aligned}$$

This is associated with the Legendre family

$$E_{\lambda,2}: \qquad z^2 = x(x+1)(x+\lambda)\ .$$

(II) If $b = 3$, we first observe that

$$\frac{1}{(n!)^2}\left(\frac{1}{3}\right)_n\left(\frac{2}{3}\right)_n\left(\frac{27}{4}\right)^n \equiv_p \binom{D}{n}\binom{2D-2n}{n}.$$

By Lemma 3.4, we obtain

$$\begin{aligned}
{}_2F_1^{(p)}\left(\frac{1}{3},\frac{2}{3};1;\frac{27}{4}\lambda\right) &\equiv_p \sum_{n=0}^{D}\binom{D}{n}\binom{2D-2n}{n}\lambda^n \\
&\equiv_p 1-\sum_{n=1}^{D}\binom{D}{n}\left(\sum_{x\in\mathbb{F}_p}x^{2D-n}(x+1)^{2D-2n}\right)\lambda^n \\
&\equiv_p -1-\sum_{x\in\mathbb{F}_p}\left[x\left(x(x+1)^2+\lambda\right)\right]^D \\
&\equiv_p \sum_{x\in\mathbb{F}_p}\left[x^3+(x+\lambda)^2\right]^D.
\end{aligned}$$

Note that we have used a change of variable $x \to \frac{\lambda}{x}$ if $\lambda \neq 0$. The associated elliptic family is

$$E_{\lambda,3}: \qquad z^2 = x^3+(x+\lambda)^2\ .$$

(III) If $b = 4$, we then note (similarly to the previous case) that

$$\frac{1}{(n!)^2}\left(\frac{1}{4}\right)_n\left(\frac{3}{4}\right)_n\left(\frac{1}{4}\right)^n \equiv_p \binom{D}{n}\binom{D-n}{n}.$$

Hence by Lemma 3.4, we find

$$\begin{aligned}
{}_2F_1^{(p)}\left(\frac{1}{4},\frac{3}{4};1;\frac{1}{4}\lambda\right) &\equiv_p \sum_{n=0}^{D}\binom{D}{n}\binom{D-n}{n}\lambda^n \\
&\equiv_p -\sum_{n=0}^{D}\binom{D}{n}\left(\sum_{x\in\mathbb{F}_p}x^{2D-n}(x+1)^{D-n}\right)\lambda^n \\
&\equiv_p -\sum_{x\in\mathbb{F}_p}\left[x\big(x(x+1)+\lambda\big)\right]^D.
\end{aligned}$$

The associated elliptic family is given by

$$E_{\lambda,4}: \qquad z^2 = x\big(x(x+1)+\lambda\big)\,.$$

(IV) If $b=6$, then using

$$\frac{1}{(n!)^2}\left(\frac{1}{6}\right)_n\left(\frac{5}{6}\right)_n\left(\frac{27}{4}\right)^n \equiv_p \binom{D}{n}\binom{D-n}{2n},$$

we obtain

$$\begin{aligned}{}_2F_1^{(p)}\left(\frac{1}{6},\frac{5}{6};1;\frac{27}{4}\lambda\right) &\equiv_p \sum_{n=0}^{D}\binom{D}{n}\binom{D-n}{2n}\lambda^n\\ &\equiv_p -\sum_{n=0}^{D}\binom{D}{n}\left(\sum_{x\in\mathbb{F}_p} x^{2D-2n}(x+1)^{D-n}\right)\lambda^n\\ &\equiv_p -\sum_{x\in\mathbb{F}_p}\left[\big(x^2(x+1)+\lambda\big)\right]^D.\end{aligned}$$

This yields the elliptic family

$$E_{\lambda,6}: \qquad z^2 = x^2(x+1)+\lambda\,.$$

Remark 5.1. The methods of this section, notably the determination that the coefficients of a given ${}_2F_1$ hypergeometric function are integers, employ the following:

Lemma 5.2. *If a, b, and n are positive integers, then*

$$\frac{b^n}{\gcd(a,b)^{2n}}\cdot\frac{\prod_{j=0}^{n-1}(a+bj)}{n!}$$

is also an integer.

The case $a=1$ was shown in [SMA09]. We give the full proof of Lemma 5.2 in the Appendix.

5.3. A note on ${}_2F_1\left(\frac{1}{4},\frac{3}{4};1;*\right)$

Let $\{E_\lambda\}$ be the family of elliptic curves defined as

$$E_\lambda : y^2 = (x-1)\left(x^2-\frac{1}{\lambda+1}\right), \qquad \lambda\in\mathbb{F}_p\backslash\{0,-1\}. \tag{5.3.1}$$

The family $\{E_\lambda\}$ is just the same as that considered in [AOP02]. We express the number of $\mathbb{F}_p$-rational points of members of the family $\{E_\lambda\}$ in terms of the natural truncation of a hypergeometric function. As before, we set $D=\frac{p-1}{2}$. The counting function I_λ for the elliptic family $\{E_\lambda\}$ is defined as

$$I_\lambda := \sum_{x\in\mathbb{F}_p}\left[(x-1)\left(x^2-\frac{1}{\lambda+1}\right)\right]^D. \tag{5.3.2}$$

Lemma 5.4. *Let $E=\lfloor\frac{D}{2}\rfloor$. The function I_λ satisfies*

$$I_\lambda \equiv_p -2^D\ {}_2F_1^{(p)}\left(\frac{1}{4},\frac{3}{4};1;\frac{\lambda}{1+\lambda}\right),$$

and the truncation of ${}_2F_1^{(p)}$ occurs at E.

Proof. We perform the change of variable $x \to 2x+1$ in (5.3.2) to obtain

$$\begin{aligned} I_\lambda &= 8^D \sum_{x\in\mathbb{F}_p} x^D \left(x(x+1)+\frac{\lambda}{4(\lambda+1)}\right)^D \\ &= 8^D \sum_v \binom{D}{v}\left(\frac{\lambda}{4(\lambda+1)}\right)^v \sum_{x\in\mathbb{F}_p} x^{2D-v}(x+1)^{D-v} \qquad (5.4.1) \\ &\equiv_p -2^D \sum_{0\le 2v\le D} \binom{D}{v}\binom{D-v}{v}\left(\frac{\lambda}{4(1+\lambda)}\right)^v, \end{aligned}$$

by Lemma 3.4. By definition, we have for all $0 \le 2v \le D$ that

$$\begin{aligned} \binom{D-v}{v} &= \frac{1}{v!}\prod_{j=0}^{v-1}(D-v-j) \\ &\equiv_p \frac{(-1)^v}{v!}\prod_{j=v}^{2v-1}\left(\frac{1}{2}+j\right) \\ &= \frac{(-1)^v}{v!}\left(\frac{1}{2}\right)_v^{-1}\prod_{j=0}^{v-1}\left(\frac{1}{2}+2j\right)\prod_{k=0}^{v-1}\left(\frac{1}{2}+2k+1\right) \\ &= \frac{(-1)^v}{v!}\left(\frac{1}{2}\right)_v^{-1} 4^v \left(\frac{1}{4}\right)_v\left(\frac{3}{4}\right)_v. \end{aligned}$$

From the equivalence

$$\binom{D}{v} = \frac{1}{v!}\prod_{j=0}^{v-1}(D-j) \equiv_p \frac{(-1)^v}{v!}\left(\frac{1}{2}\right)_v,$$

we obtain

$$I_\lambda \equiv_p -2^D \sum_{0\le 2v\le D} \frac{\left(\frac{1}{4}\right)_v\left(\frac{3}{4}\right)_v}{(1)_v v!}\left(\frac{\lambda}{1+\lambda}\right)^v.$$

The result follows. □

6. Families of K3 surfaces and ${}_3F_2\left(\frac{1}{b}, \frac{b-1}{b}, \frac{1}{2}; 1, 1; *\right)$.

We now consider 4 families of K3 surfaces with parameter λ. These are associated with the hypergeometrics ${}_3F_2\left(\frac{1}{b}, \frac{b-1}{b}, \frac{1}{2}; 1, 1; *\right)$ with $b = 2,\ 3,\ 4$ and 6.

(I) If $b = 2$, then we see that

$$ {}_3F_2^{(p)}\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}; 1, 1; -\lambda\right) \equiv_p \sum_{n=0}^{D} \frac{(-1)^n\left(\frac{1}{2}\right)_n^3}{(n!)^3}\lambda^n \equiv_p \sum_{n=0}^{D}\binom{D}{n}^3\lambda^n. \qquad (6.0.1)$$

By Lemma 3.4, we have

$$\binom{D}{n} \equiv_p -\left(\sum_{\substack{j=0 \\ 2D \mid 2D-n+j}}^{D}\binom{D}{j}\right) \equiv_p -\sum_{x\in\mathbb{F}_p} x^{2D-n}(x+1)^D$$

and

$$\binom{D}{n} = \binom{D}{D-n} \equiv_p \left(\sum_{\substack{j=0 \\ 2D \mid D+n+j}}^{D} \binom{D}{j} \right) \equiv_p - \sum_{y \in \mathbb{F}_p} y^{D+n}(y+1)^D.$$

Hence

$$\begin{aligned} {}_3F_2^{(p)}\left(\frac{1}{2},\frac{1}{2},\frac{1}{2};1,1;-\lambda\right) &\equiv_p \sum_{n=0}^{D} \binom{D}{n} \left(\sum_{x \in \mathbb{F}_p} x^{2D-n}(x+1)^D \right) \left(\sum_{y \in \mathbb{F}_p} y^{D+n}(y+1)^D \right) \lambda^n \\ &\equiv_p \sum_{x,y \in \mathbb{F}_p} \left[x(x+1)y(y+1)(x+\lambda y) \right]^D . \end{aligned}$$

This is the counting function for the K3 family

$$X_{\lambda,2}: \qquad z^2 = x(x+1)y(y+1)(x+\lambda y), \qquad \lambda \in \mathbb{F}_p \setminus \{0,-1\}, \tag{6.0.2}$$

which is associated to the family $\{E_\lambda\}$ of elliptic curves (see (5.3.1)). The families $\{X_{\lambda,2}\}$ and $\{E_\lambda\}$ were studied together in [AOP02] in order to determine the values of λ for which $X_{\lambda,2}$ is modular.

(II) If $b = 3$, we then use the identity

$$\left(-\frac{27}{4}\right)^n \frac{1}{(n!)^3} \left(\frac{1}{3}\right)_n \left(\frac{2}{3}\right)_n \left(\frac{1}{2}\right)_n \equiv_p \binom{D}{n}^2 \binom{2D-2n}{n},$$

this being valid *a priori* for all n satisfying $3n \le 2D$, and then by extension to all $0 \le n \le D$, when both sides are congruent to zero.

For $1 \le n \le D$, we apply Lemma 3.4 to obtain

$$\binom{2D-2n}{n} \equiv_p - \sum_{y \in \mathbb{F}_p} y^{2D-n}(y+1)^{2D-2n} .$$

Hence

$$\begin{aligned} {}_3F_2^{(p)}\left(\frac{1}{3},\frac{2}{3},\frac{1}{2};1,1;-\frac{27}{4}\lambda\right) &\equiv_p -1 + \sum_{n=0}^{D} \binom{D}{n} \left(\sum_{x \in \mathbb{F}_p} x^{2D-n}(x+1)^D \right) \left(\sum_{y \in \mathbb{F}_p} y^{2D-n}(y+1)^{2D-2n} \right) \lambda^n \\ &\equiv_p \sum_{x,y \in \mathbb{F}_p} \left[x(x+1)y(xy+\lambda(y+1)^2) \right]^D . \end{aligned}$$

This is the counting function for the family of surfaces

$$X_{\lambda,3}: \qquad z^2 = x(x+1)y\left(xy+\lambda(y+1)^2\right) . \tag{6.0.3}$$

(III) If $b = 4$, then we have for $0 \le n \le D$ the identity

$$(-4)^n \frac{1}{(n!)^3} \left(\frac{1}{4}\right)_n \left(\frac{3}{4}\right)_n \left(\frac{1}{2}\right)_n \equiv_p \binom{D}{n}^2 \binom{D-n}{n},$$

so that by Lemma 3.4, we obtain

$$\begin{aligned} {}_3F_2^{(p)}\left(\frac{1}{4},\frac{3}{4},\frac{1}{2};1,1;-4\lambda\right) &\equiv_p \sum_{n=0}^{D} \binom{D}{n} \left(\sum_{x \in \mathbb{F}_p} x^{2D-n}(x+1)^D \right) \left(\sum_{y \in \mathbb{F}_p} y^{2D-n}(y+1)^{D-n} \right) \lambda^n \\ &\equiv_p \sum_{x,y \in \mathbb{F}_p} \left[x(x+1)y(xy(y+1)+\lambda) \right]^D . \end{aligned}$$

The transformation $x \to \frac{x}{y}$ then gives us the counting function of the family of surfaces

$$X_{\lambda,4}: \qquad z^2 = x(x+y)y\Big(x(y+1)+\lambda\Big). \tag{6.0.4}$$

(IV) If $b=6$, then we have for $0 \le n \le D$ that

$$(-27)^n \frac{1}{(n!)^3}\left(\frac{1}{6}\right)_n\left(\frac{5}{6}\right)_n\left(\frac{1}{2}\right)_n \equiv_p \binom{D}{n}\binom{D-n}{n}\binom{D-2n}{n},$$

so that Lemma 3.4 gives

$$\begin{aligned}{}_3F_2^{(p)}\left(\frac{1}{6},\frac{5}{6},\frac{1}{2};1,1;-27\lambda\right) &\equiv_p \sum_{n=0}^{D}\binom{D}{n}\left(\sum_{x\in\mathbb{F}_p} x^{2D-n}(x+1)^{D-n}\right)\left(\sum_{y\in\mathbb{F}_p}^{*} y^{2D-n}(y+1)^{D-2n}\right)\lambda^n \\ &\equiv_p \sum_{x,y\in\mathbb{F}_p}^{*}\left[xy\left(xy(x+1)(y+1)+\frac{\lambda}{y+1}\right)\right]^D,\end{aligned}$$

where the $\sum^*$ denotes the sum over all $y \neq -1$. After some transformations similar to the case where $b=4$, this is reduced to the counting function of the family of surfaces

$$X_{\lambda,6}: \qquad z^2 = xy\Big(x(x+y+1)+\lambda y^3\Big). \tag{6.0.5}$$

There is an algebraic criterion given in [SB85, §4] for determining that a surface $\mathscr{K}$ is K3. For the affine Weierstrass equation

$$\mathscr{K}: \qquad z^2 + a_1xz + a_3z = x^3 + a_2x^2 + a_4x + a_6,$$

where each $a_i = a_i(y) \in \mathbb{F}_p[y]$, the *Weierstrass g-invariants* are defined by the identities

(a) $g_2 := \frac{1}{12}\left[(a_1^2+4a_2)^2 - 24(a_1a_3+2a_4)\right]$

(b) $g_3 := \frac{1}{216}\left[-(a_1^2+4a_2)^3 + 36(a_1^2+4a_2)(a_1a_3+2a_4) - 216(a_3^2+4a_6)\right]$.

Precisely, the condition that $\mathscr{K}$ is a K3 surface amounts to satisfying all of the following criteria:

(1) The discriminant $\Delta := \Delta(y) = g_2^3 - 27g_3^2$ is not a constant in $\mathbb{F}_p[y]$.

(2) $\deg a_i(y) \le Ni$, and $N=2$ is the smallest such integer such that this inequality is satisfied for all $i = 1,\dots,6$.

(3) Neither $\gcd(g_2(y)^3, g_3(y)^2)$ nor $\gcd(y^{12N}g_2(y^{-1})^3, y^{12N}g_3(y^{-1})^2)$ is divisible by a 12th power of a non-constant polynomial in $\mathbb{F}_p[y]$.

For each of the families $\{X_{\lambda,b}\}$ ($b=3,4,6$), the value $\lambda=0$ will be implicitly excluded. As mentioned in [AOP02], it is already known that the family $\{X_{\lambda,2}\}$ is K3. We also have the following:

Proposition 6.1. *Each of the families $\{X_{\lambda,b}\}$ ($b=3,4,6$) is K3.*

Proof. Each of these families is in simplified Weierstrass form, hence the g-invariants may be written in simplified form as

(a') $g_2 = \frac{1}{12}\left[(4a_2)^2 - 24(2a_4)\right] = \frac{4}{3}a_2^2 - 4a_4$

(b') $g_3 = \frac{1}{216}\left[-(4a_2)^3 + 36(4a_2)(2a_4) - 216(4a_6)\right] = -\frac{8}{27}a_2^3 + \frac{4}{3}a_2a_4 - 4a_6$.

(I) If $b=3$, then

$$X_{\lambda,3}: z^2 = x(x+1)y(xy+\lambda(y+1)^2) = y^2x^3 + (y^2+\lambda y(y+1)^2)x^2 + \lambda y(y+1)^2x.$$

We perform the transformation $z \to zy$ to obtain

$$z^2 = x^3 + \left(1 + \lambda\frac{y(y+1)^2}{y^2}\right)x^2 + \lambda\frac{y(y+1)^2}{y^2}x = x^3 + \left(1 + \lambda\frac{(y+1)^2}{y}\right)x^2 + \lambda\frac{(y+1)^2}{y}x.$$

We now transform $z \to y^{-3}z$, $x \to y^{-2}x$. This yields

$$y^{-6}z^2 = y^{-6}x^3 + y^{-4}\left(1 + \lambda\frac{(y+1)^2}{y}\right)x^2 + y^{-2}\lambda\frac{(y+1)^2}{y}x,$$

whence

$$z^2 = x^3 + \left(y^2 + \lambda y(y+1)^2\right)x^2 + \lambda y^3(y+1)^2x.$$

Therefore $a_2 = y^2 + \lambda y(y+1)^2$, $a_4 = \lambda y^3(y+1)^2$, and $a_6 = 0$. Thus the degree condition (2) is satisfied when $\lambda \neq 0$. The g-invariants are

(i) $g_2 = \frac{4}{3}a_2^2 - 4a_4 = \frac{4}{3}\lambda^2y^6 + \frac{4}{3}(4\lambda^2 - \lambda)y^5 + 4(2\lambda^2 - \frac{2}{3}\lambda + \frac{1}{3})y^4 + \frac{4}{3}(4\lambda^2 - \lambda)y^3 + \frac{4}{3}\lambda^2y^2$.

(ii) $g_3 = -\frac{8}{27}a_2^3 + \frac{4}{3}a_2a_4 = -\frac{8}{27}\lambda^3y^9 + \frac{4}{9}(-4\lambda^3 + \lambda^2)y^8 + \frac{4}{9}(-10\lambda^3 + 4\lambda^2 + \lambda)y^7 + \frac{8}{3}(-\frac{20}{9}\lambda^3 + \lambda^2 + \frac{1}{3}\lambda - \frac{1}{9})y^6 + \frac{4}{9}(-10\lambda^3 + 4\lambda^2 + \lambda)y^5 + \frac{4}{9}(-4\lambda^3 + \lambda^2)y^4 - \frac{8}{27}\lambda^3y^3$.

If follows that

$$\Delta(y) = 16\lambda^2y^8(y+1)^4(\lambda y^2 + (2\lambda - 1)y + \lambda)^2,$$

which is non-constant in $\mathbb{F}_p[y]$ if $p > 2$. Hence condition (1) is satisfied. We may write

$$g_2^3 = \frac{64}{27}y^6\left[z^2 + y^4z^2 + yz(-1+4z) + y^3z(-1+4z) + y^2(1-2z+6z^2)\right]^3$$

and

$$g_3^2 = \frac{16}{729}y^6\Big[2z^3 + 2y^6z^3 + 3yz^2(-1+4z) + 3y^5z^2(-1+4z) + 3y^2z(-1-4z+10z^2) + 3y^4z(-1-4z+10z^2) + 2y^3(1-3z-9z^2+20z^3)\Big]^2.$$

As y^6 is a common factor of g_2 and g_3, inspection of the terms of lowest and highest degree in y yields (respectively) the first and second parts of condition (3) when $\lambda \neq 0$.

(II) If $b = 4$, then

$$X_{\lambda,4} : z^2 = x(x+y)y(x(y+1)+\lambda) = y(y+1)x^3 + \left(y^2(y+1) + \lambda y\right)x^2 + \lambda y^2x.$$

The transformation $x \to x(y(y+1))^{-1}$ and $z \to z(y(y+1))^{-1}$ yields

$$(y(y+1))^{-2}z^2 = (y(y+1))^{-2}x^3 + (y(y+1))^{-2}\left(y^2(y+1) + \lambda y\right)x^2 + (y(y+1))^{-1}\lambda y^2x.$$

Thus

$$z^2 = x^3 + \left(y^2(y+1) + \lambda y\right)x^2 + \lambda y^3(y+1)x.$$

Therefore $a_2 = y^2(y+1) + \lambda y$, $a_4 = \lambda y^3(y+1)$, and $a_6 = 0$. In particular, the degree condition (2) is satisfied for *any* $\lambda \in \mathbb{F}_p$. The g-invariants are

(i) $g_2 = \frac{4}{3}a_2^2 - 4a_4 = \frac{4}{3}y^6 + \frac{8}{3}y^5 + \frac{4}{3}(1-\lambda)y^4 - \frac{4}{3}\lambda y^3 + \frac{4}{3}\lambda^2y^2$

(ii) $g_3 = -\frac{8}{27}a_2^3 + \frac{4}{3}a_2a_4 - 4a_6 = -\frac{8}{27}y^9 - \frac{8}{9}y^8 + \frac{4}{9}(\lambda-2)y^7 + \frac{8}{27}(3\lambda-1)y^6 + \frac{4}{9}\lambda(\lambda+1)y^5 + \frac{4}{9}\lambda^2y^4 - \frac{8}{27}\lambda^3y^3$.

It follows that

$$\Delta(y) = 16\lambda^2 y^8 (y+1)^2 (y^2+y-\lambda)^2,$$

which is non-constant in $\mathbb{F}_p[y]$ if $p > 2$. This is condition (1). As with $b = 4$, we may write

$$g_2^3 = \frac{64}{27} y^6 (2y^3 + y^4 - y^2(-1+z) - yz + z^2)^3$$

and

$$g_3^2 = \frac{16}{729} y^6 \left[6y^5 + 2y^6 + y^3(2-6z) - 3y^4(-2+z) - 3yz^2 + 2z^3 - 3y^2 z(1+z)\right]^2.$$

The analysis is as in the case $b = 3$ for $\lambda \neq 0$.

(III) If $b = 6$, then

$$X_{\lambda,6} : z^2 = xy(xy(x+y+1)+\lambda) = y^2x^3 + y^2(y+1)x^2 + y\lambda x.$$

We transform $z \to zy$ to obtain

$$z^2 = x^3 + (y+1)x^2 + \lambda \frac{1}{y} x.$$

We now perform the same transformation as in $X_{\lambda,3}$ to obtain

$$z^2 = x^3 + y^2(y+1)x^2 + \lambda y^3 x.$$

This yields $a_2 = y^2(y+1)$, $a_4 = \lambda y^3$, and $a_6 = 0$, whence the degree condition is again satisfied for any $\lambda \in \mathbb{F}_p$. The g-invariants are

(i) $g_2 = \frac{4}{3}a_2^2 - 4a_4 = \frac{4}{3}y^6 + \frac{8}{3}y^5 + \frac{4}{3}y^4 - 4\lambda y^3$

(ii) $g_3 = -\frac{8}{27}a_2^3 + \frac{4}{3}a_2 a_4 = -\frac{8}{27}y^9 - \frac{8}{9}y^8 - \frac{8}{9}y^7 + \frac{4}{3}(\lambda - \frac{2}{9})y^6 + \frac{4}{3}\lambda y^5.$

It follows that

$$\Delta(y) = 16\lambda^2 y^9 (y^3 + 2y^2 + y - 4\lambda),$$

which is non-constant in $\mathbb{F}_p[y]$ if $p > 2$, which yields condition (1). We write

$$g_2^3 = \frac{64}{27} y^9 (y + 2y^2 + y^3 - 3z)^3$$

and

$$g_3^2 = \frac{16}{729} y^{10} (1+y)^2 (2y + 4y^2 + 2y^3 - 9z)^2.$$

As in both of the previous cases, condition (3) is satisfies provided that $\lambda \neq 0$. □

We now denote by $J_{\lambda,2}$ the counting function for members of the K3 family $\{X_{\lambda,2}\}$. A suitable relationship between $J_{\lambda,2}$ and the counting function I_λ for members of the family $\{E_\lambda\}$ (5.3.1) will allow us to count the number of rational points of $\{X_{\lambda,2}\}$ in Section 7. Indeed, we have the following:

Corollary 6.2. *If $\lambda \in \mathbb{F}_p \setminus \{0, -1\}$, then the following relation holds:*

$$J_{\lambda,2} \equiv_p (1+\lambda)^D I_\lambda^2.$$

Proof. If $p \equiv_4 3$, then $E = \frac{p-3}{4}$. By Proposition 4.2 and Lemma 5.4, we obtain

$$(1+\lambda)^{D-1} I_\lambda^2 \equiv_p {}_2F_1^{(p)}\left(\frac{3}{4}, \frac{3}{4}, 1; -\lambda\right)^2.$$

Therefore, we must show that

$${}_3F_2^{(p)}\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}; 1, 1; \lambda\right) \equiv_p (1+\lambda)\, {}_2F_1^{(p)}\left(\frac{3}{4}, \frac{3}{4}, 1; \lambda\right)^2.$$

This is analogous to Clausen's formula combined with Euler's formula (see Section 4).

The case $p \equiv_4 1$ follows in a similar way. □

Remark 6.3. We have shown here that Corollary 6.2 is a consequence of Clausen's formula. In fact, it is equivalent to it in the following sense: If the Proposition is true for all primes $p \geq 3$, then formula (4.8.1) holds for $0 \leq m \leq D$, and Clausen's formula follows. To prove Clausen's formula, it suffices to show that for any $m \geq 0$

$$\left(\frac{\left(\frac{1}{2}\right)_m}{m!}\right)^3 = \sum_{\substack{u,v,\geq 0 \\ u+v=m}} \left(\frac{\left(\frac{1}{4}\right)_u \left(\frac{1}{4}\right)_v}{u!v!}\right)^2. \tag{6.3.1}$$

For any fixed $m \geq 2$, let p be a prime number exceeding $2m$, so that for this choice of m, (4.8.1) holds. Then as discussed in Section 4.6 (see (4.8.1)), we may remove the condition $u, v \leq E$, and we conclude that p divides the difference in (6.3.1) for all primes exceeding $2m$, so that (6.3.1) holds.

Since Corollary 6.2 is equivalent to Clausen's formula, it is worthwhile to give a proof of this which is independent of Clausen's formula. This was done in [AOP02] using character sums. We provide another independent proof of this in the Appendix.

7. Elliptic families and Deuring's theorem

In Section 1, we discussed the Hasse polynomial

$$H_p(\lambda) :=_2 F_1^{(p)}\left(\frac{1}{2}, \frac{1}{2}; 1, \lambda\right) = \sum_{n=0}^{D} \binom{D}{n}^2 \lambda^n.$$

In his study of splitting, Deuring [Deu41] determined the isogeny class of an elliptic curve over $\mathbb{F}_p$ via its endomorphism ring (which was generalised by Waterhouse to abelian varieties). Via the j-invariant, the number of elliptic curves in a given isomorphism class was determined according to formulae originally obtained by Eichler for Hurwitz-Kronecker class numbers. The value sets of $H_p(\lambda)$ correspond to isomorphism classes of elliptic curves over $\mathbb{F}_p$.

We first estimate the number of curves belonging to a single $\mathbb{F}_p$-isomorphism class in the family $\{E_\lambda\}$ of (5.3.1), which is associated with the K3 family $\{X_{\lambda,2}\}$. We then do the same for each of the families $\{E_{\lambda,b}\}$ ($b = 2,3,4,6$) of Section 5. In particular, this allows us to obtain estimates for the number of $\mathbb{F}_p$-rational points for the families $\{X_{\lambda,b}\}$, for $b = 2,3,4,6$, via estimates of Lenstra [Len87] for the number of curves with a given number of $\mathbb{F}_p$-rational points.

(I) $\{E_\lambda\}$: If $\lambda_1, \lambda_2 \in \mathbb{F}_p \setminus \{0, -1\}$, then we perform the variable change $(x, y) \to (x+1, y)$ to obtain the form

$$E_{\lambda_i} : y^2 = x\left(x^2 + 2x + \frac{\lambda_i}{\lambda_i + 1}\right) \qquad (i = 1,2).$$

This yields the Weierstrass form

$$E_{\lambda_i} : y^2 = x^3 + 2x^2 + \frac{\lambda_i}{\lambda_i + 1}x \qquad (i = 1,2).$$

The elliptic curves E_{λ_1} and E_{λ_2} are isomorphic over $\mathbb{F}_p$ precisely when there exist $a, b, c, d \in \mathbb{F}_p$ with $a \neq 0$, so that the change of variables

$$(x, y) \to (a^2 x + b, a^3 y + a^2 c x + d)$$

transforms the equation of E_{λ_1} into that of E_{λ_2} [Sil86]. As E_{λ_1} and E_{λ_2} lack any linear terms in y (i.e., the curves are in simplified Weierstrass form), this criterion reduces to finding $a, b \in \mathbb{F}_p$, again with $a \neq 0$, which satisfy the three identities

$$2a^2 = 2 + 3b, \tag{7.0.1}$$

$$\frac{a^4\lambda_2}{\lambda_2+1} = \frac{\lambda_1}{\lambda_1+1} + 4b + 3b^2 \tag{7.0.2}$$

$$0 = \frac{b\lambda_1}{\lambda_1+1} + 2b^2 + b^3. \tag{7.0.3}$$

In particular, equation (7.0.3) implies that $b = 0$ or $b = -1 \pm \sqrt{1 - \frac{\lambda_1}{\lambda_1+1}}$. To simplify notation, we denote these values of b as $0, \alpha, \beta$.

(I) If $b = 0$, then by equation (7.0.1), we find $a = \pm 1$, and hence by equation (7.0.2), we obtain $\frac{\lambda_2}{\lambda_2+1} = \frac{\lambda_1}{\lambda_1+1}$, so that $\lambda_1 = \lambda_2$.

(II) If $b \in \{\alpha, \beta\}$, then equation (7.0.1) uniquely determines a^2 in terms of b. Application of equation (7.0.1) to (7.0.2) yields

$$\begin{aligned}
\frac{1}{4}\left[4 - \frac{\lambda_1}{\lambda_1+1} + 2b\right]\lambda_2 &= \frac{1}{4}\left[4 + 4b + b^2\right]\lambda_2 \\
&= \left[1 + b + \frac{1}{4}b^2\right]\lambda_2 \\
&= \left[\left(1 + \frac{3b}{2}\right)^2 - 2(b + b^2)\right]\lambda_2 \\
&= \left[\left(1 + \frac{3b}{2}\right)^2 - \left(\frac{\lambda_1}{\lambda_1+1} + 4b + 3b^2\right)\right]\lambda_2 \\
&= \frac{\lambda_1}{\lambda_1+1} + 4b + 3b^2.
\end{aligned}$$

This gives a unique value for λ_2 in terms of λ_1 and the value of b, except if $4 - \frac{\lambda_1}{\lambda_1+1} + 2b = 0$. As $b \in \{\alpha, \beta\}$, we obtain

$$4 - \frac{\lambda_1}{\lambda_1+1} + 2\left(-1 \pm \sqrt{1 - \frac{\lambda_1}{\lambda_1+1}}\right) = 0.$$

This implies that $(\frac{\lambda_1}{\lambda_1+1})^2 = 0$, and hence that $\lambda_1 = 0$. This is impossible, as by definition, $\lambda \in \mathbb{F}_p \setminus \{0, 1\}$ for each member of the family $\{E_\lambda\}$. Thus λ_2 is uniquely determined by λ_1 and the value of b.

It follows that each $E_{\lambda_1} \in \{E_\lambda\}$ is $\mathbb{F}_p$-isomorphic to at most two other curves in the family $\{E_\lambda\}$.

(II) $\{E_{\lambda,b}\}$, $b = 2$: This is precisely the family of Legendre elliptic curves. Thus according to the j-invariant, there exist at most 6 elements of this family in a given $\mathbb{F}_p$-isomorphism class. See also [FW11], which calculates precisely the number of classes of $\mathbb{F}_p$-isomorphic curves for this family (their calculation is also valid over $\mathbb{F}_q$).

(III) $\{E_{\lambda,b}\}$, $b = 3$: This family is given by

$$E_{\lambda,3} : y^2 = x^3 + (x + \lambda)^2 = x^3 + x^2 + 2\lambda x + \lambda^2.$$

As with the family $\{E_\lambda\}$, the members of the family $\{E_{\lambda,3}\}$ are already in simplified Weierstrass form, whence $E_{\lambda_1,3}$ is isomorphic to $E_{\lambda_2,3}$ if, and only if, there exist $a,b\in\mathbb{F}_p$ such that $a\neq 0$,

$$a^2 = 1+3b, \tag{7.0.4}$$

$$2a^4\lambda_2 = 2\lambda_1 + 2b + 3b^2, \tag{7.0.5}$$

and

$$a^6\lambda_2^2 = \lambda_1^2 + 2b\lambda_1 + b^2 + b^3. \tag{7.0.6}$$

By equation (7.0.4), $a=\pm\sqrt{1+3b}$, and the equations (7.0.5) and (7.0.6) may therefore be read as

$$(2\lambda_2-3)b^2 + (12\lambda_2-2)b + 2(\lambda_2-\lambda_1) = 0 \tag{7.0.7}$$

and

$$(27\lambda_2^2-1)b^3 + (27\lambda_2^2-1)b^2 + (9\lambda_2^2-2\lambda_1)b + (\lambda_2^2-\lambda_1^2) = 0. \tag{7.0.8}$$

The intersection of the quadratic (7.0.7) and cubic (7.0.8) imply that b is either zero (whence $\lambda_2=\lambda_1$) or any root of the sextic polynomial

$$\begin{aligned} f(z) =& 239z^6 + 515z^5 + (316\lambda_1+313)z^4 - (4\lambda_1^2-444\lambda_1-25)z^3 \\ &+ (60\lambda_1^2+20\lambda_1-4)z^2 - (44\lambda_1^2+12\lambda_1)z - 12\lambda_1^2, \end{aligned}$$

and that λ_2 may be expressed uniquely in terms of b and λ_1 according to

$$\begin{aligned} \lambda_2 = \frac{1}{128(4\lambda_1^2+180\lambda_1-23)} & \\ \times \Big\{ & 239(34\lambda_1+1533)b^5 + 2(8038\lambda_1+363319)b^4 \\ & + (10744\lambda_1^2+492458\lambda_1+355139)b^3 \\ & - 4(34\lambda_1^3-1767\lambda_1^2-149028\lambda_1+5623)b^2 \\ & + 4(516\lambda_1^3+22920\lambda_1^2-16629\lambda_1-736)b \\ & - 4\lambda_1(466\lambda_1^2+21045\lambda_1+736)\Big\}. \end{aligned}$$

It follows that there exist at most 13 curves in this family belonging to the isomorphism class of a particular $E_{\lambda_1,3}$ over $\mathbb{F}_p$: the curve $E_{\lambda_1,3}$ and its transformations, corresponding to the values of b given by the above sextic and $a=\pm\sqrt{1+3b}$.

(IV) $\{E_{\lambda,b}\}$, $b=4$: This family is given by

$$E_{\lambda,4}: \qquad z^2 = x\big(x(x+1)+\lambda\big) = x^3+x^2+\lambda x.$$

As when $b=2,3$, members of the family $\{E_{\lambda,4}\}$ are in simplified Weierstrass form. Two curves $E_{\lambda_1,4}$ and $E_{\lambda_2,4}$ ($\lambda_1,\lambda_2\neq 0$) are $\mathbb{F}_p$-isomorphic if, and only if, there exist $a,b\in\mathbb{F}_p$ with $a\neq 0$ so that

$$a^2 = 1+3b, \tag{7.0.9}$$

$$a^4\lambda_2 = \lambda_1 + 2b + 3b^2, \tag{7.0.10}$$

and

$$0 = \lambda_1 b + b^2 + b^3. \tag{7.0.11}$$

Together, equations (7.0.9) and (7.0.10) imply that

$$(1+3b)^2\lambda_2 = \lambda_1 + 2b + 3b^2. \tag{7.0.12}$$

The intersection of the cubic (7.0.11) and quadratic (7.0.12) yield solutions $\lambda_2 = \lambda_1$ and

$$\lambda_2 = \frac{1 - 13\lambda_1 + 36\lambda_1^2 \pm \sqrt{1-4\lambda_1}(1-3\lambda_1)}{2(2-9\lambda_1)^2}.$$

It follows that there are at most 3 curves in this family belonging to the isomorphism class of a particular $E_{\lambda_1,4}$ over $\mathbb{F}_p$.

(V) $\{E_{\lambda,b}\}$, $b = 6$: This family is given by

$$E_{\lambda,6}: \qquad z^2 = x^2(x+1) + \lambda \ = x^3 + x^2 + \lambda.$$

As in previous cases, two members $E_{\lambda_1,6}$ and $E_{\lambda_2,6}$ of this family are isomorphic over $\mathbb{F}_p$ if, and only if, there exist $a, b \in \mathbb{F}_p$ with $a \neq 0$, so that

$$a^2 = 1 + 3b, \ \ 0 = 2b + 3b^2, \ \ a^6\lambda_2 = \lambda_1 + b^2 + b^3.$$

Together, these imply that $\lambda_2 = \lambda_1$ or $\lambda_2 = -\frac{4}{27} - \lambda_1$. It follows that there exist at most two members of the family $\{E_{\lambda,6}\}$ in a given $\mathbb{F}_p$-isomorphism class.

For a family $\mathscr{F}$ of elliptic curves, we denote by $C_{\mathbb{F}_p}(\mathscr{F})$ the number of elements of $\mathscr{F}$ in a given $\mathbb{F}_p$-isomorphism class. By the previous arguments, we have obtained the following:

Lemma 7.1. *(I) The elliptic family $\{E_\lambda\}$ of (5.3.1) satisfies $C_{\mathbb{F}_p}(\{E_\lambda\}) \leq 3$.*
(II) The elliptic families $\{E_{\lambda,b}\}$ $(b = 2,3,4,6)$ satisfy
(i) $C_{\mathbb{F}_p}(\{E_{\lambda,2}\}) \leq 6$,
(ii) $C_{\mathbb{F}_p}(\{E_{\lambda,3}\}) \leq 13$,
(iii) $C_{\mathbb{F}_p}(\{E_{\lambda,4}\}) \leq 3$, and
(iv) $C_{\mathbb{F}_p}(\{E_{\lambda,6}\}) \leq 2$.

As noted in Section 1, one might be able to prove even sharper bounds than those given in Lemma 7.1. We now give the proof of Theorem 1.1.

Proof of Theorem 1.1. By Proposition 1.9 of [Len87], following Deuring [Deu41], if $a \in \mathbb{Z}$ satisfies $|a - (p+1)| \leq 2\sqrt{p}$, then

$$\Big|\{\text{Elliptic curves } E \text{ such that } E(\mathbb{F}_p) = a\}/\sim \mathbb{F}_p\Big| \leq c\sqrt{p}\log p(\log\log p)^2,$$

for an effective constant c. Let $\alpha = \frac{1}{b}$, with $b = 2,3,4,6$. By the arguments of section 5, we have, up to multiplication by -1 and a constant multiplier on λ depending only on b, that ${}_2F_1^{(p)}(\alpha, 1-\alpha; 1; \lambda)$ is equivalent modulo p to the counting function for $E_{\lambda,b}$. Hence the result of Deuring and Lenstra may be applied to the value sets of ${}_2F_1^{(p)}(\alpha, 1-\alpha; 1; \lambda)$. By Lemma 7.1, the number of elements of $\{E_{\lambda,b}\}$ in any $\mathbb{F}_p$-isomorphism class is bounded by an absolute (and effective) constant. Thus the value sets of ${}_2F_1^{(p)}(\alpha, 1-\alpha; 1; \lambda)$ are bounded by $c'\sqrt{p}\log p(\log\log p)^2$, for an effective constant c' depending at most on b. □

We may now give a proof of Corollary 1.2.

Proof of Corollary 1.2.

(I) Using Proposition 4.8, with x replaced with $4x(1-x)$ in Proposition 4.10, we find that

$$ {}_3F_2^{(p)}\left(\frac{a}{b},1-\frac{a}{b},\frac{1}{2};1,1;4x(1-x)\right) \equiv_p {}_2F_1^{(p)}\left(\frac{a}{b},1-\frac{a}{b},1;4x(1-x)\right)^2. $$

Then the conclusions follow directly from Theorem 1.1.

(II) By combining Corollaries 4.3 and 4.5, the conclusion for the congruence $Q \equiv_p 0$ follows from the Theorem (using the fact that $\frac{x}{1-x}$ is invertible if $x \neq 0,\ 1$ modulo p, which we assume henceforth). For the congruence $Q(\alpha) \equiv_p m$ we have that $K = \frac{p-1}{b}$ if $p \equiv_b 1$, so that raising everything to the bth power in the Corollaries give us

$$ {}_2F_1^{(p)}\left(\frac{1}{b},1-\frac{1}{b},1;-\frac{\alpha}{1-\alpha}\right)^b \equiv_p Q(\alpha)^b \equiv_p m^b . $$

The result follows from Theorem 1.1 since b is bounded.

(III) This follows directly from Proposition 4.10 and the Theorem.

(IV) If $p \equiv_{2b} 1$, we have $K = \frac{p-1}{2b}$ in Proposition 4.12. Replacing x by $1-x^2$ in Proposition 4.12 and x by $\frac{x+1}{2x}$ in Proposition 4.10 gives us

$$ {}_2F_1^{(p)}\left(\frac{1}{b},\frac{1}{2},1;1-x^2\right) \equiv_p x^{2K}\ {}_2F_1^{(p)}\left(\frac{1}{b},1-\frac{1}{b},1;\frac{x+1}{2x}\right). $$

Raising to the bth power and using the argument of part (II) gives the result for $Q \equiv_p m$, with $m \neq 0$. When $m = 0$, the result follows from combining Propositions 4.12 and 4.10 without raising to powers.

□

Remark 7.2. It is also possible to interpret $J_{\lambda,2}$, the counting function for the $K3$ family $X_{\lambda,2}$ (discussed in Section 6) in terms of I_λ via zeta functions. For example, in Theorem 4.2 of [AOP02], it is shown that

$$ J_{\lambda,2} = 1 + p + 19p + \left(\frac{\lambda+1}{p}\right)_L (\pi^2 + \overline{\pi}^2 + p) \quad \text{and} \quad I_\lambda = (p+1) - (\pi + \overline{\pi}), $$

where π^{-1} is a root of the zeta function $Z(E_\lambda/\mathbb{F}_p, T)$, and that each member of $\{E_\lambda\}$ has good reduction at p. As $\pi\overline{\pi} = p$, it follows that $\pi^2 + \overline{\pi}^2 \equiv_p (\pi + \overline{\pi})^2 \equiv_p (I_\lambda - 1)^2$. (Here, $\left(\frac{\lambda+1}{p}\right)_L$ denotes the Legendre symbol). Therefore

$$ J_{\lambda,2} \equiv_p 1 + \left(\frac{\lambda+1}{p}\right)_L (I_\lambda - 1)^2. $$

This implies that $J_{\lambda,2} \equiv_p 1$ precisely when $I_\lambda \equiv_p 1$. Thus for any $a \in \mathbb{F}_p$, it follows that $J_{\lambda,2} \equiv_p a$ if, and only if,

$$ \left(\frac{\lambda+1}{p}\right)_L (I_\lambda - 1)^2 \equiv_p a - 1. $$

The latter equivalence implies that $(I_\lambda - 1)^4 \equiv_p (a-1)^2$. This implies that for any such a, there exist at most 4 numbers $a_1, \ldots, a_4 \in \mathbb{F}_p$ so that $I_\lambda \equiv_p a_i$. It is therefore natural to ask the when the surfaces $X_{\lambda,b}$ are modular for $b = 3, 4, 6$, and also whether the rank of the Néron-Severi group can be explicitly calculated. We do not pursue this question here.

8. Hypergeometric E-functions

A relative of this argument may be performed for hypergeometric E-functions. For example, the classical Kummer hypergeometric function is defined as

$$K_{\nu,\lambda}(z) = \sum_{n=0}^{\infty} \frac{(\nu)_n}{(\lambda)_n} \frac{z^n}{n!} \qquad (\lambda \neq 0, -1, -2, \ldots),$$

which satisfies the second-order differential equation $zy'' + (\lambda - z)y' - \nu y = 0$. For an element $\alpha \in \mathbb{F}_q$ ($q = p^m$), the Pochhammer product is defined as

$$(\alpha)_n = \alpha(\alpha+1)\cdots(\alpha+n-1).$$

Let $\nu \in \mathbb{F}_q$, and let λ be a rational number or an element of $\mathbb{F}_q$. The degree $N^*_{\nu,\lambda}$ of the truncation $K^{(p)}_{\nu,\lambda}(x)$ depends upon the values of λ and ν, and takes the form

$$N^*_{\nu,\lambda} = \frac{\omega_{\nu,\lambda} p - a_{\nu,\lambda}}{b_{\nu,\lambda}}.$$

We let $\eta(z) = K_{\nu,\lambda}(z^{b_{\nu,\lambda}})$. Then $\eta^{(p)}(x) = K^{(p)}_{\nu,\lambda}(x^{b_{\nu,\lambda}})$ has degree equal to $\omega_{\nu,\lambda} p - a_{\nu,\lambda}$. From the differential equation for the function $\eta(z)$ and inspection of degrees, one obtains that $\eta^{(p)}(x)$ is a solution to the differential equation

$$\frac{x}{b_{\nu,\lambda}} y'' + \left[(\lambda - x^b_{\nu,\lambda}) - \frac{b_{\nu,\lambda} - 1}{b_{\nu,\lambda}} \right] y' - b_{\nu,\lambda} x^{b_{\nu,\lambda}-1} \nu y \equiv_p 0 \mod x^{p - a_{\nu,\lambda} - 1}. \tag{8.0.1}$$

Proof of Theorem 1.4. The function $\eta^{(p)}(x)$ is a solution to equation (8.0.1) multiplied by $x^{a_{\nu,\lambda}+1}$ (a small degree relative to p) modulo x^p. By Lemma 5.1 of [GW15], if $(m+1)n^2 < p$, then the function $\eta^{(p)}(x)$ does not satisfy an equation

$$a_n(x) T^n + \cdots + a_1(x) T + a_0(x) \equiv_p 0 \mod x^p,$$

where $a_i(x) \in \overline{\mathbb{F}}_p[x]$ and $\deg(a_i(x)) \leq m$ for all $i = 1, \ldots, n$ [GW15, Lemma 5.1]. By Siegel's argument (see §II.10 of [Sie49], Theorem 1.3 of [GW15], or Lemma 2 of [Shi11]), it is not hard to show that if a polynomial P in two variables over $\overline{\mathbb{F}}_p[x]$ is of sufficiently small degree such that $P(\eta^{(p)\prime}(x), \eta^{(p)}(x)) \equiv_p 0 \bmod x^p$, then there exists a solution y^* to the reduced Kummer equation whose logarithmic derivative is algebraic over $\overline{\mathbb{F}}_p(x)$, also of small degree. Precisely, this solution is found by aggregating the (homogeneous) terms of highest total degree in P as a function H, and for two linearly independent solutions y_1, y_2 to Kummer's differential equation, choosing $y^* = c_1 y_1 + c_2 y_2$ so that $H(c_1 y_1' + c_2 y_2', c_1 y_1 + c_2 y_2) \equiv_p 0$.

Expanding the Riccati equation

$$u' + \frac{\lambda - z}{z} u + u^2 \equiv_p \frac{\nu}{z}$$

for $u = y^{*\prime}/y^*$ around $x = \infty$, which exists as a Puiseux series as we have tamed ramification, gives us that the expression

$$u = \sum_{k=0}^{\infty} c_k x^{r_k}$$

with $r_0 > r_1 > \cdots$ rational powers are in fact integer powers [Shi11, Lemma 8]. By the Riccati equation, the only possible branch points of u are at $x = 0, \infty$, whence u must be a rational function in $\overline{\mathbb{F}}_p(x)$. Let $u = P_0/P_1$, where $P_0, P_1 \in \overline{\mathbb{F}}_p[x]$, $P_1 \not\equiv_p 0$. By

construction, the form $R = P_1 w' + P_0 w$ satisfies $R(y^*) \equiv_p 0$ and $x\frac{d}{dx}R(y^*) \equiv_p 0$ at the solution $w = y^*$. By comparison of degrees in x, there exist $a, b \in \overline{\mathbb{F}}_p$ such that

$$x\frac{d}{dx}R \equiv_p (ax+b)R.$$

This yields two differential equations in terms of P_0 and P_1:

$$P_1' - \left(\frac{\lambda+b}{x} + a - 1\right)P_1 + P_0 \equiv_p 0,$$

and

$$P_0' - \left(\frac{b}{x} + a\right)P_0 + \frac{\nu}{x}P_1 \equiv_p 0.$$

There are four possible cases: $a \equiv_p 0$ or $a \equiv_p 1$ and $\lambda + b \equiv_p 0$ or $\lambda + b \not\equiv_p 0$. We note that if $a \equiv_p 0$, then $\deg(P_0) = \deg(P_1)$. We let a_i denote the coefficient of x^i for P_0, and b_i the same for P_1. This pair of differential equations yields the following result.

(I) If $a \equiv_p 0$ and $\lambda + b \equiv_p 0$, then by the first differential equation, the largest $m < p$ for which the coefficient of x^m in P_1 is nonzero is the same as that for P_0, and for this m, $a_m + b_m \equiv_p 0$. By the second differential equation, we have $\nu - \lambda \equiv_p m$.

(II) If $a \equiv_p 0$ and $\lambda + b \not\equiv_p 0$, then $b \equiv_p 0$, as P_0 and P_1 are relatively prime. With m the same as the previous case, it follows that $\nu \equiv_p m$.

(III) If $a \equiv_p 1$ and $\lambda + b \equiv_p 0$, then again for the largest $m < p$ such that the coefficient of x^m in P_1, is nonzero, $a_{m-1} + m b_m \equiv_p 0$. As the largest such nonzero coefficient for P_0 is equal to $m-1$ by the first differential equation, we have $-a_{m-1} + \nu b_m \equiv_p 0$. Hence $\nu \equiv_p -m$.

(IV) If $a \equiv_p 1$ and $\lambda + b \not\equiv_p 0$, then by the first differential equation, we have that $x | P_1$. As P_0 and P_1 are relatively prime, we have as in case (2) that $b \equiv_p 0$. Also by the first differential equation, we have $m b_m - \lambda b_m + a_{m-1} \equiv_p 0$. Also, $-\lambda b_p + a_{p-1} \equiv_p 0$ and, by the second differential equation, $-a_{p-1} + \nu b_p \equiv_p 0$. If $a_{p-1} \not\equiv_p 0$, then $-\lambda \equiv_p -\nu$, whence $\lambda = \nu$. If $a_{p-1} \equiv_p 0$, then as $\lambda, \nu \not\equiv_p 0$, $b_p \equiv_p 0$. It follows that the largest $m < p$ for which the coefficient of x^m in P_1 is nonzero is again one more than that for P_0, and thus for this m that, by the second differential equation, $-a_{m-1} + \nu b_m \equiv_p 0$. Thus $\lambda b_m - m b_m \equiv_p a_{m-1} \equiv_p \nu b_m$, whence $\lambda - m \equiv_p \nu$. Thus $\lambda - \nu \equiv_p m$.

In any case, we have that $\nu \in \mathbb{F}_p$ from (II) and (III) or $\lambda - \nu \in \mathbb{F}_p$ from (I) and (IV). If λ and ν are chosen so that $\nu, \lambda - \nu \notin \mathbb{F}_p$, we obtain a contradiction. We let A denote the maximal degree of the coefficients of P and B the total degree of P in its two variables. Via an auxiliary polynomial $\Phi(x, \eta^{(p)}(x), x^p, \eta^{(p)'}(x))$, we must choose C and D simultaneously so that

$$[2(A+1)B+1](2B^2)^2 < p \quad \text{and} \quad D(A+C+2D) < \frac{AC(B+2)}{2}.$$

We let $A = \delta\lfloor p^{2/7} \rfloor$, $B = C = \delta\lfloor p^{1/7} \rfloor$, $D = \delta^3 \lfloor p^{2/7} \rfloor$, and $\varepsilon = \frac{1}{7}$. (See [HB96] or [GW15]; the denominator of 7 is a general feature of second-order differential equations of this kind.) Hence the number of solutions $\lambda \in \mathbb{F}_p$ to the congruence $\eta^{(p)}(\lambda) \equiv_p 0$ is bounded by $(A + (p-1)B + pC)/D \ll_\delta p^{1-\varepsilon}$. □

Suppose that $m \geq 2$ and y_0 is a solution of minimal degree to an algebraic differential equation of the form

$$y^{(m)} + Q_{m-1} y^{(m-1)} + \cdots + Q_1 y' + Q_0 y = R \tag{8.0.2}$$

with $R, Q_0, \ldots, Q_{m-1} \in \mathscr{L}$, a field of analytic functions (over $\mathbb{C}$) which is closed under differentiation. As in [Shi11, Lemma 11, §6], if $P \in \mathscr{L}[x_1, \ldots, x_m]$ and $P(y_0, y_0', \ldots, y_0^{(m-1)}) = 0$, then there exists a solution y^* to (8.0.2) such that the terms P_s of highest total degree in P satisfy $P_s(y^*, y^{*\prime}, \ldots, y^{*(m-1)}) = 0$. Theorem 1.4 is the case $m = 2$ over $\mathbb{F}_p$. If $m = 3$, then the solution y^* satisfies a Riccati differential equation in terms of P. It is very interesting to consider whether results of this type hold for differential equations of order greater than two.

9. Appendix

Here, we give a proof of Corollary 6.2 which does not use Clausen's formula. This proof has some features in common with the proof of Theorem 4.2 of [AOP02]; however, we dispense with character sums and provide some simplifications.

Proof of Corollary 6.2. By definition of $J_{\lambda,2}$, we write

$$J_{\lambda,2} = \sum_{l=0}^{D} \binom{D}{l} S(2D-l,D)S(D+l,D)\lambda^l.$$

For all of the terms in this sum with $l \neq 0$, Lemma 3.4 applies, so that we may write

$$J_{\lambda,2} \equiv_p S(2D,D)S(D,D) + \sum_{1\leq l\leq D} \binom{D}{l}^3 \lambda^l.$$

As $S(2D,D) \equiv_p S(D,D) \equiv_p -1$, it follows that $J_{\lambda,2} \equiv_p \sum_{l=0}^{D} \binom{D}{l}^3 \lambda^l$. We perform the change of variables $\mu = -\frac{\lambda}{1+\lambda}$ ($\mu \neq 0,-1,\infty$, $\lambda \neq 0,-1,\infty$), so that

$$J_{\lambda,2} \equiv_p (1+\lambda)^D \sum_{l=0}^{D} \binom{D}{l}^3 (\mu+1)^{D-l}(-\mu)^l.$$

Let us write $\binom{D}{l}^2 = \binom{D}{l}\binom{D}{D-l}$, and we recognise this product as the coefficient of $x^l y^{D-l}$ of $(1+x)^D(1+y)^D$, and hence the coefficient of $x^D y^D$ of $x^{D-l}(1+x)^D y^l(1+y)^D$. Therefore $J_{\lambda,2} \equiv_p (1+\lambda)^D J^*_{\lambda,2}$, where $J^*_{\lambda,2}$ is the coefficient of $x^D y^D$ of

$$(1+x)^D(1+y)^D \sum_{l=0}^{D} \binom{D}{l} (x(\mu+1))^{D-l}(-\mu y)^l = (1+x)^D(1+y)^D[x+\mu(x-y)]^D.$$

We write $x-y = (1+x)-(1+y)$, and we expand the previous sum in terms of powers of μ to obtain

$$\sum_{m=0}^{D} \binom{D}{m} \mu^m \sum_{r=0}^{m} \binom{m}{r} (1+x)^{D+r} x^{m-r} (1+y)^{D+m-r} (-1)^{m-r}.$$

Isolating the coefficient of $x^D y^D$ yields via Corollaries 3.2 and 3.3 that

$$J^*_{\lambda,2} \equiv_p \sum_{m=0}^{D} \left(\frac{-\mu}{4}\right)^m \binom{D-m}{m} \sum_{r=0}^{m} \binom{m}{r} \binom{D+r}{m} \binom{D+m-r}{D} (-1)^r.$$

By definition, $\binom{m}{r}\binom{D+r}{m} = \binom{D+r}{D}\binom{D}{m-r}$. Replacement of r with $m-s$ yields

$$J^*_{\lambda,2} \equiv_p \sum_{m=0}^{D} \left(\frac{\mu}{4}\right)^m \sum_{s=0}^{m} (-1)^s \binom{D+s}{s} \binom{D}{s} \binom{D+m-s}{D} \binom{2D-m}{m}.$$

We have

$$\binom{D}{s}\binom{D+m-s}{D}\binom{2D-m}{m} = \binom{D+m-s}{m}\binom{2D-m-s}{m-s}\binom{2D-m}{s}.$$

By Lemma 3.1, we also have

$$\binom{D+s}{s} = \binom{2D-(D-s)}{s} \equiv_p (-1)^s \binom{D}{s}$$

and

$$\binom{D+m-s}{m} \equiv_p (-1)^{D+s}\binom{2D-m}{D-s}.$$

Therefore

$$J^*_{\lambda,2} \equiv_p (-1)^D \sum_{m=0}^{D}\left(\frac{\mu}{4}\right)^m \sum_{s=0}^{m}\binom{2D-m}{s}(-1)^s\alpha_{m,s}, \tag{9.0.1}$$

where $\alpha_{m,s} = \binom{2D-m-s}{m-s}\binom{2D-m}{D-s}\binom{D}{s}$ is the coefficient of $x^{m-s}y^{D-s}z^s$ in $(1+x)^{2D-m-s}(1+y)^{2D-m}(1+z)^D$, and thus the $x^{2D}y^Dz^D$ coefficient of

$$[x(1+x)(1+y)]^{2D-m}(z(1+z))^D\left(\frac{xy}{(1+x)z}\right)^s.$$

In the sum over s, if $s > m$, then the power of x exceeds x^{2D} and thus contributes nothing. Therefore, we may extend the sum, which gives us the $x^{2D}y^Dz^D$ coefficient of

$$[x(1+x)(1+y)]^{2D-m}(z(1+z))^D\left(1-\frac{xy}{(1+x)z}\right)^{2D-m}$$

for the sum over s. The substitution $z \to \frac{1}{z}$ and multiplication by z^{2D} yields the $x^{2D}y^Dz^D$ coefficient of

$$[x(1+x)(1+y)]^{2D-m}(1+z)^D\left(1-\frac{xyz}{1+x}\right)^{2D-m}.$$

We now make the following sequence of changes of variables:

(i) $z \to \frac{z}{1+y}$, multiply by $(1+y)^D$; the $x^{2D}y^Dz^D$ coefficient of

$$[x(1+x)]^{2D-m}(1+y+z)^D\left[1+y-\frac{xyz}{1+x}\right]^{2D-m}.$$

(ii) $y \to \frac{1+z}{y}$, multiply by $(1+z)^{-D}y^{2D}$; the $x^{2D}y^Dz^D$ coefficient of

$$[x(1+x)]^{2D-m}[y(1+y)]^D\left[1+\frac{1+z}{y}\left(1-\frac{xz}{x+1}\right)\right]^{2D-m}.$$

(iii) $z \to -\frac{z}{x}$; the $x^Dy^Dz^D$ coefficient of

$$(-1)^D[x(1+x)]^{2D-m}[y(1+y)]^D\left[1+\frac{1}{y}\left(1-\frac{z(z+1)}{x(x+1)}\right)\right]^{2D-m}.$$

Computing the y^D coefficient, then the z^D coefficient, and finally the x^D coefficient, we find that the sum over s is equivalent modulo p to

$$(-1)^D\sum_{r=0}^{D}\binom{2D-m}{r}\binom{D}{r}\sum_{u=0}^{r}\binom{r}{u}\binom{u}{D-u}\binom{2D-m-u}{m+u-D}(-1)^u.$$

We now let $v = D-u$ and interchange the sums, which yields

$$\sum_{v=0}^{D}(-1)^v\binom{D-v}{v}\binom{D-(m-v)}{m-v}\sum_{r=D-v}^{D}\binom{D}{r}\binom{2D-m}{r}\binom{r}{D-v}. \tag{9.0.2}$$

As $\binom{D}{r}\binom{r}{D-v} = \binom{D}{v}\binom{v}{D-r}$, the sum over r is equal to

$$\binom{D}{v}\sum_{r=D-v}^{D}\binom{2D-m}{r}\binom{v}{D-r} = \binom{D}{v}\binom{2D-m+v}{D},$$

which by Lemma 3.1 is equivalent modulo p to $(-1)^{m+v+D}\binom{D}{v}\binom{D}{m-v}$. Substitution into (9.0.2) and (9.0.1) then yields

$$J_{\lambda,2} \equiv_p (1+\lambda)^D \sum_{m=0}^{D} \left(\frac{\lambda}{4(1+\lambda)}\right)^m \left[\sum_{v=0}^{m} \binom{D-v}{v}\binom{D-(m-v)}{m-v}\binom{D}{v}\binom{D}{m-v}\right]$$
$$= (1+\lambda)^D \left[\sum_{v=0}^{D} \binom{D}{v}\binom{D-v}{v}\left(\frac{\lambda}{4(1+\lambda)}\right)^v\right]^2.$$

The result follows using (5.4.1). □

We now give a proof of the claim in Lemma 5.2.

Proof of Lemma 5.2. It suffices to show that

$$b^n \cdot \frac{\prod_{j=0}^{n-1}(a+bj)}{n!}$$

is an integer when $\gcd(a,b)=1$, for all $n \in \mathbb{N}$. Via Legendre, we have at a prime integer p,

$$v_p(n!) = \sum_{k=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

In particular, let $p|b$ and $v_p(b)=m$. Thus by Legendre we also have

$$v_p(n!) = \frac{n - s_p(n)}{p-1} \leq n \leq mn = v_p(b^n),$$

where $s_p(n)$ denotes the sum of the base-p digits of n. As the product $\prod_{j=0}^{n-1}(a+bj)$ is relatively prime to b, it follows that

$$v_p\left(b^n \cdot \frac{\prod_{j=0}^{n-1}(a+bj)}{n!}\right) \geq 0.$$

Let us now consider the case where $p|a$. We then have

$$v_p\left(b^n \cdot \frac{\prod_{j=0}^{n-1}(a+bj)}{n!}\right) = v_p\left(\frac{\prod_{j=0}^{n-1}(a+bj)}{n!}\right).$$

Furthermore,

$$v_p\left(\frac{\prod_{j=0}^{n-1}(a+bj)}{n!}\right) = v_p\left(\prod_{j=0}^{n-1}(a+bj)\right) - v_p(n!).$$

By Legendre's formula, we again have

$$v_p(n!) = \sum_{k=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

We find similarly for Pochhammer's factorial $\prod_{j=0}^{n-1}(a+bj)$. We have $a+bj \equiv bj \bmod p$, and as $\gcd(p,b)=\gcd(a,b)=1$, the element $a+bj$ is divisible by p precisely when $j|p$. It follows that

$$\left|\left\{a+bj \;\middle|\; j=0,\ldots,n-1,\ p|a+bj\right\}\right| = \left\lfloor \frac{n-1}{p} \right\rfloor + 1 \geq \left\lfloor \frac{n}{p} \right\rfloor.$$

Similarly, if $k \geq 2$, then $p^k|a+bj$ precisely when j is of the form

$$j = \frac{\lambda p^k - a}{b} \in \mathbb{Z},$$

and j is of this form precisely when $p^k | a + b(j + p^k)$, so that every p^kth element of $a + bj$, $j = 0, \ldots, n-1$ is divisible by p^k. It follows that

$$\left| \left\{ a + bj \;\middle|\; j = 0, \ldots, n-1,\ p^k | a + bj \right\} \right| \geq \left\lfloor \frac{n}{p^k} \right\rfloor.$$

As in the proof of Legendre's theorem, every additional power of p dividing $a + bj$ contributes once to the p-adic valuation of the Pochhammer product. We thus have

$$v_p\left(\prod_{j=0}^{n-1} (a + bj) \right) \geq \sum_{k=1}^{\lfloor \log_p(a+b(n-1)) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor \geq \sum_{k=1}^{\lfloor \log_p(n) \rfloor} \left\lfloor \frac{n}{p^k} \right\rfloor = v_p(n!).$$

Let us now consider a prime $p \nmid a, b$. As with $p | a$, we have

$$v_p\left(b^n \cdot \frac{\prod_{j=0}^{n-1}(a + bj)}{n!} \right) = v_p\left(\frac{\prod_{j=0}^{n-1}(a + bj)}{n!} \right).$$

We note that the valuations decompose as

$$\begin{aligned} v_p\left(\frac{\prod_{j=0}^{n-1}(a + bj)}{n!} \right) &= v_p\left(\prod_{j=0}^{n-1} (a + bj) \right) - v_p(n!) \\ &= v_p\left(\prod_{j=0}^{n-1} (a + bj) \right) - v_p\left(\prod_{j=0}^{n-1} (1 + j) \right). \end{aligned}$$

In this case, p^k divides $j + 1$ if, and only if, $j = l p^k - 1$, and p^k divides $bj + a$ if, and only if, $j = l p^k - \alpha_k$, $\alpha_k \in \{1, \ldots, p^k - 1\}$, $\alpha_k b \equiv a \bmod p^k$. It follows that

$$\begin{aligned} v_p\left(b^n \cdot \frac{\prod_{j=0}^{n-1}(a + bj)}{n!} \right) &= \sum_{j=0}^{n-1} \left[v_p(a + bj) - v_p(1 + j) \right] \\ &= \sum_{k} \left\lfloor \frac{n - 1 + \alpha_k}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^k} \right\rfloor \geq 0. \end{aligned}$$

We have thus proven for all prime integers p that

$$v_p\left(b^n \cdot \frac{\prod_{j=0}^{n-1}(a + bj)}{n!} \right) \geq 0,$$

and therefore that

$$b^n \cdot \frac{\prod_{j=0}^{n-1}(a + bj)}{n!}$$

is an integer, as desired. □

References

[AOP02] S. Ahlgren, K. Ono, and D. Penniston, *Zeta functions of an infinite family of K_3 surfaces*, Amer. J. Math. **124** (2002), no. 2, 353–368.

[BM04] J. Brillhart and P. Morton, *Class numbers of quadratic fields, hasse invariants of elliptic curves, and the supersingular polynomial*, J. Num. Th. **106** (2004), 79–111.

[BT14] C. Brav and H. Thomas, *Thin monodromy in $Sp(4)$*, Compositio Mathematica **150** (2014), no. 3, 333–343.

[Deu41] M. Deuring, *Die typen der multiplikatorenringe elliptischer funktionenkörper*, Abh. Math. Sem. Hamburg **195** (1941), 197–292.

[FMS14] E. Fuchs, C. Meiri, and P. Sarnak, *Hyperbolic monodromy groups for the hypergeometric equation and Cartan involutions*, J. Eur. Math. Soc. **16** (2014), 1617–1671.

[FW11] R. Feng and H. Wu, *On the isomorphism classes of Legendre elliptic curves over finite fields*, Sci. China Math. **54** (2011), no. 9, 1885–1890.
[GW15] A. Ghosh and K. Ward, *The number of roots of polynomials of large degree in a prime field*, Int Math Res Notices **4** (2015), 898–926.
[HB96] D.R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, Analytic Number Theory: Proceedings of a Conference in Honor of Heini Halberstam (1996), 451–63.
[Len87] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. Math. **126** (1987), no. 3, 649–673.
[Mah76] K. Mahler, *Lectures on transcendental numbers*, Springer, 1976.
[Ole68] V A Oleinikov, *On the transcendence and algebraic independence of the values of certain entire functions*, Math. of the USSR-Izvestiya **2** (1968), no. 1, 61–87.
[SB85] J. Stienstra and F. Beukers, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3 surfaces*, Math. Ann. **271** (1985), 269–304.
[Shi11] A. Shidlovskii, *Transcendental numbers*, De Gruyter, 2011.
[Sie49] C.L. Siegel, *Transcendental numbers*, Princeton U. Press, 1949.
[Sil86] J.H. Silverman, *The arithmetic of elliptic curves*, Springer, 1986.
[Sin15] S. Singh, *An extended list of arithmetic monodromy in $Sp(4)$*, arXiv:1502.07529 (2015).
[SMA09] A. Straub, V.H. Moll, and T. Amdeberhan, *The p-adic valuation of k-central binomial coefficients*, Acta. Arith. **140** (2009), 31–42.
[SV14] S. Singh and T. N. Venkataramana, *Arithmeticity of certain symplectic hypergeometric groups*, Duke Math. J. **163** (2014), 591–617.
[Tak77] K Takeuchi, *Arithmetic triangle groups*, J. Math. Soc. Japan **29** (1977), no. 1, 91–106.

AMIT GHOSH, Department of Mathematics, Oklahoma State University, Stillwater, OK 74078, USA *E-mail address*: ghosh@okstate.edu

KENNETH WARD, Department of Mathematics & Statistics, American University, Washington, DC 20016, USA *E-mail address*: kward@american.edu